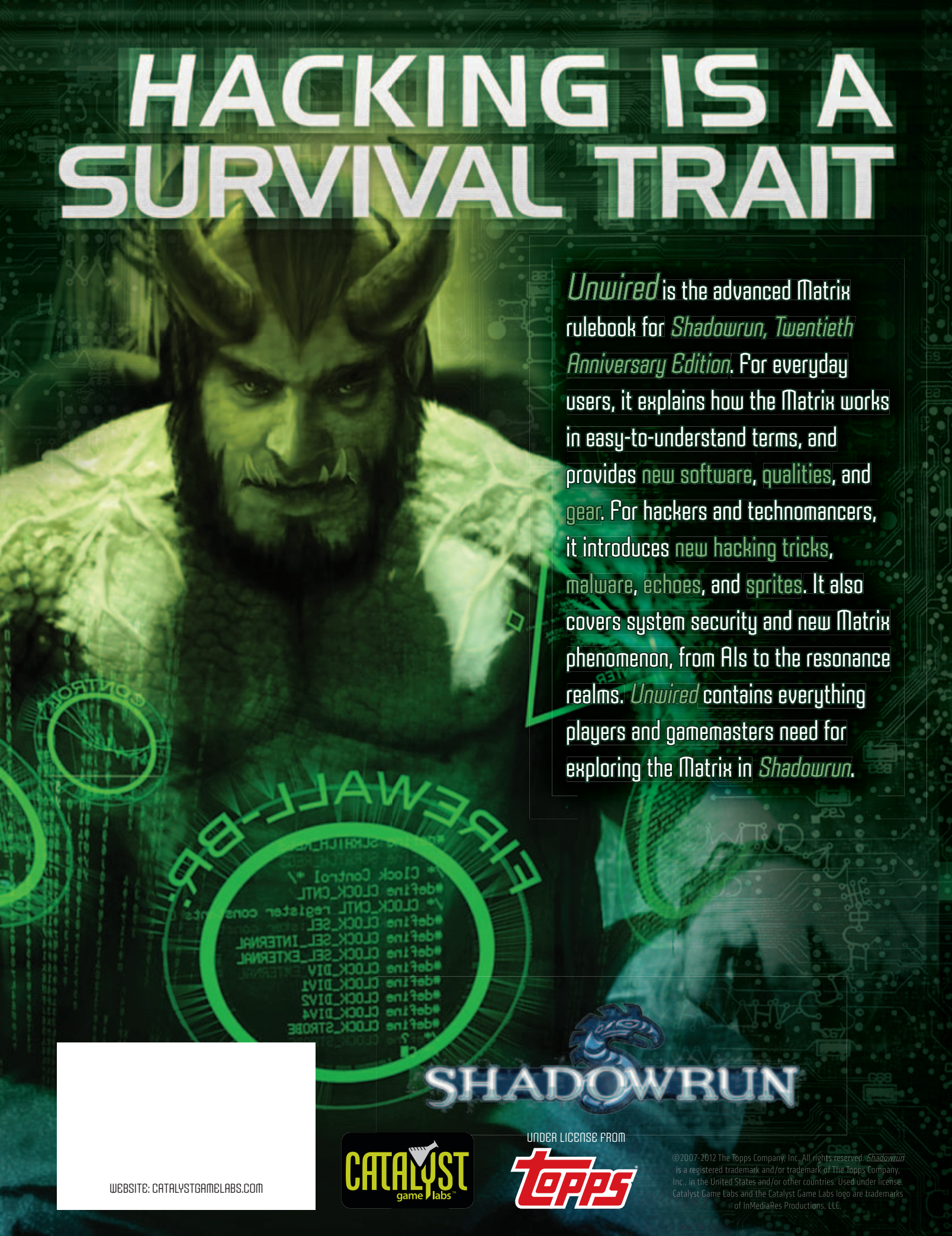
# SHADOWRUN

# UNWIRED

CATALYST game labs™

CORE MATRIX RULEBOOK

# HACKING IS A SURVIVAL TRAIT



*Unwired* is the advanced Matrix rulebook for *Shadowrun, Twentieth Anniversary Edition*. For everyday users, it explains how the Matrix works in easy-to-understand terms, and provides new software, qualities, and gear. For hackers and technomancers, it introduces new hacking tricks, malware, echoes, and sprites. It also covers system security and new Matrix phenomenon, from AIs to the resonance realms. *Unwired* contains everything players and gamemasters need for exploring the Matrix in *Shadowrun*.

SHADOWRUN

UNDER LICENSE FROM

WEBSITE: CATALYSTGAMELABS.COM


UNWIRED
WARNING!
CHECK ENGINE
TOMORROW'S WEATHER
77/45 QUAKE WARNING
ACCIDENT REPORTS
• avoid the corner of 6th & main
• gas leak on Woodward at 4th
• 5 car accident with fatality on North Ave west of Clybourn
D
P
40 MPH
catalyst Game labs

# . . . TABLE OF CONTENTS . . .

## SIDEBARS



# CREDITS: UNWIRED

**Writing:** Lars Blumenstein, Rob Boyle, Robert Derie, Jennifer Harding, Martin Janssen, Ralf Koehler, Jay Levine, Moritz Lohmann, Sascha Müller, Aaron Pavao
**Editing:** Rob Boyle, Andrew Hackard, Jason Hardy, Robyn King-Nitschke, Michelle Lyons
**Development:** Rob Boyle, Peter Taylor
**Art Direction:** Randall Bills
**Interior Layout:** Jason Vargas, Matt Heerdt
**Cover Art:** Klaus Scherwinski
**Cover Layout:** Matt Heerdt
**Illustration:** Mariusz Gandzel, Philip Hilliker, Régis Moulun, Chad Sergesketter, Tony Shasteen, Eric Williams
**Inspiration:** Tonikom and 100blumen (dev-editing music), 2600 magazine, security guru Bruce Schneier, haxploitation movies
**Shout-Outs:** All the folks who contributed to previous Shadowrun Matrix books: *Virtual Realities, Virtual Realities 2.0, Matrix, Target: Matrix, Renraku Arcology: Shutdown, Brainscan, Threats 2,* and *System Failure.* Thanks also to Mikael Brodu, Masaaki Mutsuki, Adam Jury, Olivier Thieffine, Stephan Wodkowski, Tobias Wolter, and all of the playtesters for ideas and/or feedback.
**Playtesters:** Natalie Aked, Rob Aked, Sarah Baker, Tony Bruno, Chuck Burhanna, Steven A. Carroll, Jean-Marc Comeau, Andrew Coen, Joanna Craven, Marc Dagenais, Benjamin Davenport, Craig Engle, Rachel Engle, Cullen Erbacher, Doug Fleming, Eric Fleming, Bruce Ford, Eugen Fournes, Jason Freese, Nick Garden, Kendall Jung, Jason Keats, James O'Laughlin, David Lundquest, Chris Maxfield, Greg Nielsen, Aaron Pavao, Bryan Pow, Lyall Pow, Richard Riessen, Grant Robinson, Jonathon Staite, Eva Schiffer, Doug Smith, Pat Smith, Steve Smith, Mark Somers, Adam Taliscka, Lee Thoms, Tom Tuckerman, John Unchelenko, Luc Villeneuve, Jeremy Weyand, Mark Young, Leland Zavadil and Michael Zenke



Third Printing, corrected,
by Catalyst Game Labs,
an imprint of InMediaRes Productions, LLC
PMB 202 • 303 - 91st Ave. NE, E-502
Lake Stevens, WA 98258.

Find us online:
info@shadowrun4.com
(Shadowrun questions)
http://www.shadowrun4.com
(official Shadowrun website)
http://www.catalystgamelabs.com
(Catalyst website)
http://www.battlecorps.com/catalog
(online Catalyst/Shadowrun orders)

Connecting Jackpoint VPN ...
... Matrix Access ID Spoofed.
... Encryption Keys Generated.
... Connected to Onion Routers.
> Login
**********
> Enter Passcode
**********
... Biometric Scan Confirmed.
Connected to <ERROR: NODE UNKNOWN>
*"The urge to destroy is a creative urge."*

**Welcome back to Jackpoint, omae; your last connection was severed: 1 hour, 50 minutes, 1 second ago**


## *JACKPOINT STATS*

**57 users currently active in the network**

**Latest News**
* <ERROR> Newsfeed currently unavailable.

**Personal Alerts**
* Your messages have all been erased.
* Your Agent Smithers has crashed. Restart? Y/N
* Your Agent Scully is reporting impaired operability.
* Your processor limit is at 97% capacity

**First Degree**
<ERROR> First Degree currently unavailable

**Your Current Rep Score:** 57 (95% Positive)

**Current Time:** May 09, 2071, 2218

PREFERENCES
FEEDS
TASKS
LINKS
HISTORY

## *COMSTAR FIREWALL ALERT*

Your commlink defenses have been breached by an unknown intruder.
Offensive Countermeasures Initiated.
Trace Initiated.
Jackhammer Loaded.
Do You Wish to Engage? Y/N

### Trace Initiated

... Proxy Server Identified. [Details]
... Initiating Proxy Server Traffic Analysis

Danger! Your PersOnn85#2d.....[{
0a3d0d
&&&^^^^^12e958>:.09
56fdd8 *&Dc8d * CY&DSgt
FDSSFDds87
... ERROR ///

CHAT | MESSAGES | FILES | POSTS | NEXUS | SEARCH


## *UNWIRED*

**Invited Guests**
Otaku-Zuku Inbus

**Posts/Files tagged with "Unwired":**
* Idiot's Guide to the Matrix
* Hacker's Handbook
* Technomancers
* Matrix Phenomena
[More]

CONTINUE
ADVANCED SEARCH
SAVE

# . . . MATRIX OVERVIEW . . .

"Hello! Would you like to try our New! Iced! Mocha! with Genuine! Chocolate! flavoring?" The AR waitstaff popped up as soon as I sat down in the mall café's chair, like the RFID tag in the plastic seat was just waiting for my ass to connect with the cushion. I sent my order to the café: Soy-kaf, black. My bank account dropped by two nuyen, bringing it perilously close to zero. Shit.

A couple of tables down, my mark settled in. The way his brown eyes were flicking around like ping-pong balls on crack, I could tell he was multi-tasking on his 'link. He had something in his hand—another goddamned commlink. When'd he pick that up? Damn him for being smart enough to have a second 'link, not to mention picking this busy mall to make his call. I'd hacked his normal 'link earlier and found nothing. Now I knew why.

I bit my lip, trying to decide—hack or scan? Must be two hundred 'links nearby. If I didn't have some proof of his suspected infidelity by tonight, I'd lose this job. Rent was due on the first. The room wasn't much, but miss a payment and the damn door would be locked, the appliances shut off, all my settings—like that Virtual Window I'd splurged on—remotely destroyed by the software that ran the building. The software I could handle. It was my big-ass ork landlord I didn't want to short change.

A human waitress slammed my coffee on the table, moving off towards customers who looked like better tip prospects—like my mark, with his 4,000 nuyen suit and fancy haircut. I sighed and began sorting through the wireless chatter.

"Oh my God, did you see—"

"No, I'm so not—"

"Mooooommmm—"

"Those shoes—"

"Hot chick, ten o'clock—"

Damn. The guy's eyes had stopped their frantic motion. He was smiling into space. Got to go faster.

I flicked through the babble, desperate to catch his call before he finished. Ah, here's one. Encrypted. Not your teeny-bopper mallrats. I unleashed my decryption prog, counting the seconds as I took a sip of the overpriced soy-kaf. Watched as his handsome face—which cost more than I made in a year, no doubt—smirked. My program beeped as it broke the encryption. I began recording.

"Honey, you know I can't. The witch is watching me 24-7. I think she's hired someone . . . . Baby, just one more month and the prenup is over . . . " His voice was smooth, cultured, dripping with sex appeal—the best modern technology could provide. "I promise, baby. The very second. 'Til then, let's just keep it virtual . . . ."

I had to admit he was slick. I'd spent a week watching him with no sign of a honey, not a single moment when I couldn't account for his whereabouts. Now I knew why. Lucky for my client, divorce courts had ruled a couple years ago on online affairs. Looked like the bastard wouldn't be making his prenup after all.


EW
08

## MATRIX AND EVERYDAY LIFE

» A couple of us here on Jackpoint have been discussing this collection for a while now. Seems like everyone's always going off on the Awakened world or talking about the newest and biggest guns. While I'll agree that magic is something every runner better take into account, the Matrix is gonna be a lot more relevant to the average runner, wage slave or squatter than any discussion of magic. Astral space is accessible only to a select few, but virtual space is accessible to everyone, everywhere, for only the price of hardware. It's 2071 and metahumanity has created a whole new world. Let's go for a tour.
» Pistons

Those of us in the shadows can be pretty far out of touch with the average Joe on the streets. It never hurts to know what the wageslaves of the world are doing, though; today's innocent bystander is tomorrow's mark. To that end, I've gathered some info on everyday life for those people who actually live within the law.

Most people never venture past the superficial levels of the Matrix, considering it little more than a venue for increased virtual socialization, more convenient shopping, on-demand entertainment, and, of course, work. Communication is key here, since it is the primary way most people talk to their friends, their bosses, their colleagues, even their families.

Back before the Crash, most homes had a central cyberterminal. It was an all-in-one computer, trid, phone/email service, message center, simsense ... everything. Now that cyberterminal has been condensed into a personal commlink that's carried with you everywhere, all the time, connecting you to the AR world 24/7. With today's faster-than-thought transmission speeds, there are no global barriers any more. The Matrix is the ultimate way to bring your life up to speed and let you live it to the fullest. You can read your gossip news in one AR screen, have directions guide you to the nearest coffee shop in another AR window, and be talking to someone in Singapore in a third. Once upon a time you'd see someone walking down the street and talking to themselves, and you'd figure they'd lost it. Now you can walk down any urban street and you'll see crowds of people, AR glasses on, holding conversations with people only they can see or hear. Sure, you get your folks with built in 'links, mostly older folk who just can't quite seem to go with the flow and act like raving lunatics with the rest of the youngsters. Among the 16–25 demographic, though, datajacks and internal 'links are just so "2060-ish"—or so I've been told.

» With the recent technomancer scare, people with internal commlinks were frequently targeted by ignorant, fearful crowds. Even those of us with internal 'links started carrying a commlink to avoid that danger.
» Glitch

Another side-effect of the AR communication change is that people mostly use their icons as their virtual representation. Used to be you had to be sitting in front of your cyberterminal or staring into the tiny screen/camera of your pocket secretary to have a video-enabled conversation with someone around the globe. Now, unless you're willing to walk around, carrying a camera pointed to your face while you talk, your icon is what the other person sees, not your face.

The technology exists to create a virtual "you," a perfect representation of yourself complete with mannerisms and personal quirks, and use it as your icon. That was all the rage a few years back. The newest fashion, though, is to use customizable "personas," like Horizon's Perfect Fit, which allows a user to create an idealized version of themselves. Since so many people interact solely in cyberspace, why not be exactly who you want to be? Nowadays a voice-only call is unusual, limited to shady business deals and paranoid shadowrunners.

### BUSINESS

The business world was crippled in the aftermath of the crash. As a result, when the Matrix was rebuilt, the service providers ensured it could never crash again (or so they'd like us to believe), building a web of wireless coverage that blankets most metro areas. Given the damage done to hardware and the infrastructure, it quickly became obvious that rebuilding—much less maintaining—the old-fashioned wired telecom system wasn't profitable. Now most corps have jumped fully on the wireless bandwagon. It's quick, easy, and profitable—for them and for us.

Through AR, employees can be logged in from home, from the road, or even from nomadic work environments. Virtual offices are considered convenient, quick to set up, and most importantly cost-efficient. With no central offices, wageslaves become their own mobile offices, eliminating the costs of maintaining central buildings, increasing the amount of hours an employee can be available, and ensuring business can run 24/7/365.

» The security holes in this business approach leave room for enterprising criminals like us. Want to hack into a secure network? Just drop in to visit Bob-the-Accountant at home, log on through his system, and Voila! Big corps often house their employees in secure corporate enclaves to thwart such efforts, making this approach a bit more complicated.
» Glitch

» For the real sensitive stuff, though, like those juicy R&D specs for that new drone you're drooling over, corps lock everything—and everyone—down in a secured building or campus.
» Slamm-O!

» Don't fool yourselves into thinking you're getting away with something when you take advantage of a security hole like that. Corps account for "shrink"—losses from theft, data breaches, and other sources—just like any other line item on their budget. They also tend to be proactive in managing those losses when the bottom line is threatened.
» Mr. Bonds

Other corporations provide fully jacked-in offices where wageslaves go, plug in, and then spend the next twelve hours in a VR office, with no outside distractions to hamper full productivity. In high security areas, the system may be completely off line with employees required to "check" their personal commlinks at the door and use a workplace 'link while on site. Naturally, this does lead to a high number of burnout employees, but hey, people are replaceable, right?

Businesses have also discovered the ease of using AR for training, monitoring employees, and disseminating corporate

bullshit. AR transmissions are so easy to eavesdrop on, employees in the new AR world have no privacy at work or at home. Most wageslaves have no idea of how closely their corporate masters are watching. I certainly am not going to be the one to break the news.

AR technology has also allowed corporations to better deploy their personnel in dangerous or difficult environments, such as mining, underwater environments, and even construction. By using RFID tags and AR, corporations can reduce risk through constant surveillance of every worker, warning him of dangerous zones, preventing entry into unsecured areas, and monitoring vital signs and productivity.

» More and more corporations are taking cheap (read: disposable) labor and slapping some shoddy skillwires into them, creating workers overnight. It makes for great flexibility, since the corp can download new skills/training into their workforce at any time. Much more cost-efficient than investing years of training, education, and time into employees.
» Aufheben

» The skillwires are substandard, the healthcare non-existent, and the corp charges the employee for the cost of the surgery and gear, taking it out of their wages. The employee is an unpaid slave for months, if not years, once they tack on interest and all the extra costs of care, upgrades, and routine maintenance.
» Nephrine

» I don't know what's worse, seeing so many sign away their bodies and souls just to survive on the pitiful wages offered, or seeing even more of the unskilled workers displaced by the fully automated factories and cheap drone labor that so many corps rely upon, leaving metahuman workers with the choice between polluting their bodies or watching their families starve.
» Fatima

» Drones are easy to build, easy to control, and you don't get the costly screw-ups inherent in a metahuman workforce. It's the way of the world. If the poor SOBs want to get out, they can. I did.
» Butch

» While the ethics lecture is entertaining, I'd rather spend my time productively. Drone workforces are a fact of life. A smart runner knows how to use them to his advantage. If your hacker can get into the system, they can control the place. Talk about a great advantage.
» 2XL

» Shit, what's scary is that some of these places have security hackers and riggers on duty. Nothing worse than getting a team into a place only to realize there's a spider—a security rigger—who can jump into the security system and "become" the building. A few weeks back I got into a lab full of skillwired grunts and an alarm got set off. While our hacker was fighting through the building's system and the rest of us were trying to deal with the security drones, the damn spider downloaded a new set of skillsofts into the grunts. Transformed the bunch from lab grunts to trained security forces. In a matter of seconds, we had 100-plus orks who suddenly knew a hell of a lot about kicking our asses. Needless to say, we left.
» DangerSensei

## WHO ARE YOU?: I.D. IN THE WIRELESS WORLD

Your System Identification Number is a unique identifier issued to you at birth or any time you change national or corporate citizenship. This identifier (which is not just alpha-numeric) contains basic information, such as your birthdate, birthplace, and other data, encoded within the identifier. If issued at birth, your SIN will be linked to basic biometric data, such as a DNA sample, retinal scan, and finger prints. As you age, additional biometrics such as voice patterns, facial patterns, and hand measurements can be added. Your SIN is registered with your country or corporation of citizenship as well as with the Global SIN Registry. Following the Crash, most governments and corporations began requiring multiple backup databases that can be accessed in case of national emergency.

Your **ID** contains all the data necessary to interact with other citizens, government/corporate agencies, and physical or online retailers. Although every issuing country/corp embeds different data on a citizen's ID, they generally contain your name, age, metatype, a physical description, a current photo, licenses, and are frequently linked to your bank account. Many countries also require IDs to contain your status if you are Awakened or a technomancer along with registries of any cyber- or bioware you have.

Your SIN is linked to biometric data and proves you are a citizen. Your ID is who you are. Together, they allow you to exist in today's world.

The other big business interest in AR is selling stuff to all those wageslaves (and you). Lots and lots of stuff. With the ability to track every purchase you make, real-time. Every store you enter, every restaurant you patronize, right down to the soymilk you added to your coffee this morning … well, let's just say, the system knows more about you and your preferences, than you do. It didn't take long for corporations to realize what a lucrative business market-data tracking is. There's some seriously heavy competition out there for your buying patterns, and everyone with a SIN and disposable income is targeted. You walk down the street and get bombarded with restaurants reciting their daily specials, stores advertising sales of your preferred brand of underwear, street side vendors blasting you with viral ad-software, entertainment parlors flashing neon AR signs to get your attention … it is impossible to escape the constant data assault in any commercial center. Any time you actually show interest in one of the ads, your attention is noted and compiled with the rest of your consumer profile. Corporate interests have ensured that turning your commlink to

hidden mode (or chucking it into the nearest recycler) is suspicious or illegal, and will almost always get you noticed by police or security forces. For the average Joe on the street, the constant ad-war is a simple fact of life. For runners, however, I'd highly recommend that if you begin to have personalized ads sent your way, it is a sure sign that it's time to chuck your current ID and buy a new one.

## HOME

The home of your average Joe is a fully networked, fully controlled AR-enhanced environment managed through a central node that is linked to the resident's commlink. If the fridge unit detects that the soy milk is getting sour, the central home management software notifies your commlink, which then orders a grocery delivery, pays through automatic debit from your bank account, and even sends your kid a reminder note to dump the old milk down the sink when he gets home from soccer practice. More affluent homes will skip the kid part, of course, since those critters are notoriously unreliable, and simply tell the home drone to perform the task. Homes in more modern apartment buildings, neighborhoods, and corporate enclaves are designed to take care of all those pesky homeowner responsibilities like scheduling regular maintenance, monitoring systems like plumbing or HVAC, and automatically requesting repairs or upgrades from authorized service providers. You've got a problem with your laundry machine? The machine notifies the central home management software, which asks you to approve the repair charges then authorizes a repair tech to your home, who is allowed access to your home when he approaches with his work-order and service ID (stored, obviously, on his commlink), all while you're out enjoying yourself shopping for more gadgets.

» Of course, poor neighborhoods have few, if any, of these amenities. And the really high class neighborhoods and buildings have actual metahumans running the systems, so don't expect to get away with the "water-heater repair guy" act in those places without some serious prep work.
» Ma'fan

Drones are also common in most homes. The middle class is especially fond of household drones, which can take care of the cleaning, home maintenance, and other home chores. Drones can be toys for your kids, pets for your family, or even provide security for your home. The drones are generally controlled through the home's central node and home management software. After the events of the last year, drones have gotten a bad rap, but the corps are pushing back with heavy advertising on how safe, efficient, and "unhackable" the new generation of drones are.

» "Unhackable?" What a laugh. I've used drones to open doors, record incriminating videos, place drugs in beverages and food, even to give a particularly annoying asshole food poisoning (by having a home service drone leave some ham out at room temperature for too long then serve it up in a sandwich).
» Glitch

» That's not counting the fact that you can use home drones to attack people—even if it's just the little vacuuming drone tripping someone as they walk by the stairs … .
» Slamm-O!

In addition, AR connected interior design programs are very popular, allowing a user to customize wallpaper or carpet patterns, change lighting and music options, even alter the views out of a window. For those who prefer to live a totally augmented life, a variety of AR image overlays exist, providing virtual artwork, virtual image overlays for furniture and appliances, virtual pets, even virtual roommates for those who want them. I've walked into places and seen writhing dragons where the sofa should be, sat on squat gargoyles instead of chairs, and met the most annoying virtual hellhound puppies. The only limits are imagination and the depth of your bank account (good taste, apparently, is *not* a limiting factor in many decorating schemes).

Home entertainment has also blossomed with AR. If your daughter wants to watch the newest VirtualWorldDisney cartoon crap while your son wants to see the latest "Nathan Never" sim, your wife wants to watch a celebrity gossip show, and you want to zone out to some quiet tunes, you can all do so while sharing the comfort of your own living room. There are numerous entertainment services that advertise as "family friendly," meaning they offer multiple feeds for each person in the household. If you choose AR or full VR immersion, you can have your entertainment of choice blasting your senses without bothering your family or neighbors.

» Speaking from experience, I'm much happier when my son blows out his eardrums virtually rather than making me listen to the crap he calls music.
» Snopes

» And I'm even happier when I can immerse *myself* in something to ignore the rest of my family.
» Sounder

» Careful there, Sounder. I've walked right through a room full of people, all too busy being entertained to even notice me. I *love* AR.
» Mika

## EDUCATION

Education has jumped on the AR bandwagon for better or worse. School districts in the poorer areas have switched to educational software, tutor-agents, and virtual teachers for many of their hard-to-staff schools. For the cost of one teacher's salary, you can provide 400 kids with second-hand commlinks and knock-off AR goggles. Literacy rates in the UCAS are at an all time low, as the written word has gone sadly out of style. It's totally possible today for a kid to get a low-end job without being able to read or write, since universal icons, verbal instructions, and easy user-interfaces dominate the workplace.

Personally, I think this trend is a major contributor to the divide between the have and have-nots, since higher education, well-paying employment, and advancement is blocked for so much of society. Of course, in affluent areas, or for the favored corporate citizens, education is enhanced by the availability of AR. Specialized teachers from around the globe can lecture to hundreds at a time, advanced coursework can be taught through interactive software, and advanced degrees can be attained without ever stepping foot on a physical college campus.

Corporations, the government, and military operations have embraced virtual training simulations. SWAT and special ops teams can link up in virtual reality to train for any situation, from urban combat zones to extreme weather conditions. A friend hooked me up with an arctic training mod, run hot-sim, full VR, and I swear, after I jacked out of that program, I had to check to make sure I hadn't frozen any important bits of myself off. I've also heard about task-specific training, pre-op stuff that allows a team to run through a virtual representation of a building or combat zone, to, say, prep for a hostage recovery operation or a high-risk infiltration. From what I've seen, this tech is mostly limited to corporate black-ops teams and specialized military applications. Still, I know a few runners who've, ah, acquired a copy of the tech, and they swear by it.

## ELECTRONIC FUNDS

Money these days is nothing more than bits of electrons, shuttled between virtual banks with an implied agreement to honor the dataflow. During the Crash 2.0, that system was severely shaken up. The fallout bankrupted banks and common folk alike. In the last five years, a new system has evolved. It used to be that you could use your credstick to make purchases or transfer money. Perfect for us shadow folks, since certified credsticks made a great anonymous money system. Now, everyone utilizes their commlink. Registered credsticks are almost obsolete, unfortunately, gone the way of past human monetary systems like shells, gems, gold, and paper currency. A lot of stores don't even carry credstick readers anymore. That means that to interact with the legitimate world and do anything from hopping on a bus to purchasing a new helicopter, you need to have a commlink with a valid SIN hooked up to a valid bank

Urgent Message...

» Hey, with all this useful, factual info floating around, I feel the urge to contribute. I know none of the intelligent, skeptical, rational folk here on JackPoint believe this shit, but that doesn't mean that the brain-dead masses don't. Enjoy.
» Snopes

» If you want to "discuss" these, *please* take it off here and go to Snopes' site.
» FastJack

### MATRIX URBAN LEGENDS

**The Black Chip Killer:** A mysterious black chip that circulates from user to user. When you slot it, you don't see much of anything. Without you realizing it, though, the soul of a serial killer captured on the chip uploads into your brain. While you sleep that night, the killer rises from your dreams, takes over your body, and goes on to kill more victims. He continues killing until he's caught, or killed, but either way, he downloads himself into another chip and disappears ... leaving you unaware of anything your body has done, waking up to a nightmare of prison, or even death, for murders you don't remember.

**Ghosts in the Machine:** People who die while connected to the Matrix have their minds trapped online. They may only live for a few minutes or for eternity. Sometimes you can hear lost ones screaming as they search endlessly for their body.

**Split Personality:** While in surgery for a datajack, your surgeon inserts a sleep regulator without your knowledge. He also downloads the memories of another person, who bribed him to find her a new body. When you fall asleep, the sleep regulator kicks in and the other person wakes up, in control of your body. Strange clues haunt you, like finding your things rearranged or meeting people on the street who call you by another name, until one day you realize you're not alone ... .

**The Carjacking:** When driving, you see an oncoming vehicle flash its headlights at you. Annoyed, you flash your headlights back, not realizing this is a hacker-gang initiation. The new ganger must hack the first car they can get to respond and either cause it to crash or force it to drive to an area of town where the gangers wait to ritualistically slaughter the trapped passengers (and then go joyriding in their new vehicle).

**Hacker Revenge:** An egotistic man bumps into a scrawny little guy and is incredibly rude, bullies the kid, or insults the kid's race (depending on the story). A week later, the man begins to have problems with his commlink. His bank account doesn't verify funds, his house won't open for him, even his car

***Continued on page 13***


account. Makes life a bit harder for those of us who prefer not to leave a data trail, but there are ways around it.

For the average Joe, the entire system is convenient and practically invisible. His paycheck is deposited into his account electronically. The government gets first dibs, with taxes automatically calculated, filed, and paid promptly, without any thought from Joe. After that, his regular bills are paid, set up for automatic debits that don't require any attention on Joe's part. When Joe catches the bus to work in the morning, the bus fare is automatically paid via his commlink—same thing for the soy-kaf he grabbed from the street vendor at the bus stop. All of these transactions take place real-time, and smart consumers utilize money-management software to ensure they don't overextend themselves.

» Registered credsticks may be out, but you can still use (and misuse) certified credsticks. Most banks will accept them and they do provide a measure of security, since it allows shadowy folks like us to hide our cash transactions. Or if you're truly paranoid, many of the grey-market banks will issue anonymous credit and ID tokens.
» Mr. Bonds

» ID tokens?
» Sticks

» Anonymous ID tokens are basically a statement issued by a bank that says you've verified your ID with them, and they're vouching for your ID and cred. Let's say you want to buy a medkit. You don't want to worry about having your data harvested by some corporate marketing bots or ID thieves. So you slot your ID token from the Malaysian Independent Bank at the online sales store. Your token says 'yes, she's a real person and authorized to purchase this item.' Nothing else. No name, no SIN, nada. The credit is transferred and you've left no data trail ... I'm sure you can see how sweet this really is. You'll find it at the shadier banks, for us criminal types, and at the really high-roller institutes, for all those super-rich who can afford privacy.
» Mr. Bonds

» Yeah, but you won't see wageslaves walking around with them, which means you'll get some funny looks if you try to use them in person. Now for online transactions, they work just fine. If you want to blend, though, you better load some of that nice anonymous cred onto your 'link and accept the data trail.
» Pistons

» In many areas, SINless workers are paid in certified cred (if not by barter), allowing those barrens area sweat-shops to thrive. Of course, there's almost no way they can use their hard-earned money legitimately. Grey market shops and gang-controlled 'distribution networks' accept cert cred almost exclusively. Subsistence-level barter systems are also common.
» Fatima

» In some backwater places they still do use corp script, archaic metal, or paper currencies, or even trade in items of value, be it gold, telesma, medical supplies, or whatever. If you plan travel outside of the sprawls, be sure to check what type of currency to bring.
» Traveler Jones

## THE AUGMENTED WORLD

The augmented world has been designed to appeal to consumers' desire for instant gratification, simplicity, and ease of use. Most wireless users adapted quickly to having multiple screens of data displayed, allowing us to satisfy our short-attention spans and need for instantaneous news, music, entertainment, whatever we desire. Global AR coverage means you can talk to anyone, anywhere, anytime. AR-enhanced products like clothing, makeup, and body augmentations mean we never have to make due with the boring, mundane world. Virtual clubs, societies, and communities ensure that you'll meet like-minded folks around the globe, even if you never meet in the flesh. For many users, the virtual world has become more real—and certainly more interesting and fulfilling—than the unaugmented world.

Daily life is constantly augmented. People view the world through their AR glasses or cybereyes, using the AROs that guide them through the streets, enjoying or ignoring the constant barrage of advertisements, and watching streaming news or gossip feeds. Look at other people crowding around you and you'll see their augmented appearance—perhaps they are wearing clothes embedded with AR functionality, changing a plain bodysuit into a swirling mass of colors and textures when viewed through AR. Makeup and hair/skin products do similar things. Cover your face with AR-enhanced makeup and your features will change into anything you can imagine. Hair can be transformed into writhing masses of snakes or colors never seen in nature.

Socially, more and more people are turning to the virtual world to find companionship and romance. Dating networks (and the spam they inundate us with) are more common than fish in the sea. In the last few years, many countries including the UCAS have granted legal status to virtual marriages (and virtual divorces). Which means that you can meet your true love online, run off to virtual Las Vegas, get hitched in a virtual Church of Elvis ceremony, and then enjoy a virtual honeymoon.

- And then be virtually surprised when your cute 25-year-old hot blonde woman turns out to be a hairy 38-year-old man.
- Snopes

- Been burned with some online dating, eh?
- Netcat

- What happens in VR stays in VR. Heh.
- Slamm-0!

### KNOWLEDGE AT YOUR FINGERTIPS

Perhaps the most useful benefit of the augmented world is the ability to instantaneously access information. Someone references an obscure speech by a 1960's civil rights leader at a meeting? Send out a search with a few keywords, and within seconds you can have the entire speech, a Cliff's Quickie™ version, several relevant commentaries on the social and economic impact, a life history for the speaker ... you get the point. Interested in purchasing a new vehicle? Send a search out and get nearby dealerships, competitive price quotes, consumer ratings, safety test-ratings, reliability guides, and blogs of recent owners detailing their experiences with the same make and model. Curious about that cute guy across the mall? Read his profile, see he loves combat biking, and search for recent biking news while you walk over. By the time you're next to him, you can have a perfect opening line.

Searching for information is intuitive, simple, and (generally) low-cost. Anyone can do a basic search—the commlink and software do all the work. There's really no reason to be ignorant. And it isn't simply "book" knowledge stored on the Matrix. You can search for information on cultures, customs, proper etiquette, slang, even current bribe rates. You can hear native speakers giving courteous (or rude) greetings, watch examples of gang hand-language, or see step-by-step instructions on proper Japanese tea ceremony etiquette (with live instruction, in case you're at a meeting and don't want to offend with your lack of manners).

**MATRIX URBAN LEGENDS *(CONT.)***

refuses to start with his biometric key. Then his SIN disappears from the UCAS registry... eventually the cops find him, wandering the streets, wearing apparently "stolen" clothes. When they run his prints, they find a long criminal history with several outstanding warrants. As the man is roughly pushed into the cop car, he catches sight of the scrawny kid watching. The kid looks him in the eye and flips him the bird.

**Brain Cancer:** Wireless signals cause brain cancer. Luckily, you can download your memories and soul onto a chip, and then upload them again into a healthy clone brain. No foul, no harm.

**The Exchange:** This mysterious social network links shadowrunners across the globe via untraceable commlinks that they generally find among their possessions without any warning. The links are always marked with a distinctive red X. Runners who obey the requests issued by the link (anything from a major run to giving a squatter a ride somewhere, or even more inane things like leaving a flashlight on a park bench at a certain time) find themselves rewarded; those who disobey, punished. The legend says the Exchange is really run by an AI, but what no one knows is what its agenda is.

Urgent Message...

MATRIX OVERVIEW

## MATRIX COMMUNITIES/CULTURE

The Matrix is a vibrant environment created by us metahumans, so where better to meet and socialize with others of our kind? Whatever your tastes, from sharing information to perusing porn, from gathering with intellectuals to bashing someone's virtual brains out in the latest Neil the Ork Barbarian game, you can find it on the Matrix. Everyone can find a place to fit in. Which may be why the Matrix is the fastest growing community out there—is, in fact, perhaps the only community for many sprawl citizens.

### SOCIAL NETWORKS

Folks have been using the Matrix to socialize for longer than even FastJack's been alive. With AR, social networks have taken the next step, allowing you to meet people, virtually or in person,

who fit your own personally tailored specs. Interested in a certain cause? Fanatic about an AR game? Just want to pick up cute chicks? Or perhaps you're interested in the latest celebrity gossip or political muckraking? Social networks bring people together from all around the globe—and beyond, these days—to support a common cause. From terrorists to VR gamers, social gossipers to consumer rights advocates, everyone uses these networks to gather and disseminate information. While many are harmless blog-fests, others attempt to change society through public awareness. A few have become real thorns in corporate and government sides, but their widespread appeal, large memberships, and decentralized networks make them almost impossible to shut down. Members can upload video footage and files, post blogs, and meet up in virtual chatrooms to discuss issues. Some are private, but many are open to anyone.

Especially popular right now are the geosocial networks, also called Mobile Social Software or MoSoSos, which can provide up-to-the-minute tracking of others in your network, or simply notify you when someone from your network is nearby. For groups that allow users to post schedules, MoSoSos can even provide projected times when a member may be within range of your protected area, so members can meet up. Want to know what clubs other members of your MoSoSo are going to be hitting tonight? Perhaps you're at the mall and see that someone else from your *Rocky Mountain Avatar* game is nearby, and want to challenge him to an AR duel? Creepy for those of us in the shadows, but hugely popular with busy wage-slaves wanting to cram as much socializing as possible into their precious non-working hours.

Private Message...

### A MESSAGE FROM FASTJACK. READ IT. OR ELSE.

» A quick reminder for everyone on my rules for JackPoint. I created this system to help disseminate knowledge through the runner community. Everyone here was invited because they have something valuable to share. Lurking is allowed but your rep will benefit more if you share.

I've only got a few rules. Break 'em and you're off the system.

1. Don't hack JackPoint.
2. Don't try to trace anyone from JackPoint.
3. Anyone loading malware onto JackPoint—intentionally or otherwise—will be tracked down and beaten.

If you've got a problem with someone, use the rep system. Don't complain to me unless they've broken one of the above rules. I didn't create this network to become a father to fifty-eight whining toddlers, so if you want to squabble, keep it off here. Ditto if you and someone hit it off ... but send an occasional recording for a lonely old man. ;)
» FastJack

» Jack, you are such a letch.
» Kat o' Nine Tales

## MATRIX GANGS AND TRIBES

Matrix gangs, unlike their physical world counterparts, can be based anywhere in the world with members in different cities or even continents. Since the gear and warez cost nuyen, a lot of Matrix gangs are made up of affluent, rebellious kids trying to piss off mommy & daddy rather than trying survive the streets. Gangs focus on matrix crimes, ranging from AR vandalism to software piracy and smuggling. Recent trids out of LA have glamorized gangs online and off, so new wannabes have sprung up everywhere.

» Annoying little buggers. They can be a real problem for most users, but if you've got a decent attack prog and some skill, you can whip their obnoxious asses back to their cushy basements.
» Slamm-0!

» Some are more than just annoying. The Electric Knights made headlines last month when they managed to hack the grid-link system in Seattle and caused some massive pileups on I-5. Three dead and a few dozen hospitalized.
» FastJack

Most Matrix gangs rely on numbers and brute strength, not talent, but that's enough to harass and exploit small time mom-and-pop virtual storefronts and be a nuisance to normal Matrix users. A popular gang trick is a take on the old protection racket, where the gang offers "protection" to a business—often from a homemade virus—and then unleashes the virus if the business refuses to pay. These gangs trade on their victims' lack of Matrix knowledge to keep them cowed. Organized crime gets into the picture, too—several Seoulpa rings are entirely virtual or focused on virtual crimes, like the Choson Ring in Seattle.

Matrix tribes are on the other end of the spectrum, formed by people—hackers, technos, and wannabes—looking for protection, friendship, and a sense of connection and belonging. Tribes can be simple, based on religion, ethnicity, or race. They might even by based on common interests like the Family Play Tribe based in Seattle, whose members join to arrange virtual playdates for their kids, or on exceptional abilities like the Ravens, a technomancer tribe based out of the PCC grid. In just a few years, sometimes only months, the tribes develop their own customs, iconography, and even languages. Most sponsor at least one dedicated node with members-only access. The Ravens, for example, have a private Kiva accessible through the PCC's public KivaNet.

» The Ravens had their node established long before the PCC created KivaNet. I've heard it is actually a Resonance well, attuned to their tribe.
» Netcat

## REP SYSTEMS

We've all heard of Horizon's P2.0, their highly marketed reputation "system of the stars." But Horizon didn't invent the idea—although they certainly seem to have made the most money off of it. Back when online social networks were just beginning,

people started cobbling together reputation systems to go with them. Online market places had buyers providing reputation scoring for the sellers to help encourage honest sales practices. Online social networks allowed users to recommend or blacklist other users. Our own Jackpoint utilizes a basic rep system, where we each can add or subtract rep points from other users. If any one of us gets out of hand, the rest of us can punish him or her by dropping their rep score. At some point, Jack might even drop them from the network.

» No one gets dropped unless they break the rules. I'm not the police. You can certainly base your interactions on someone's rep score, though. Peer pressure is a wonderful thing.
» FastJack

Most online marketplaces use a rep system of some sort. Legal marketplaces like **The Bazaar** connect buyers and sellers, tracking transactions through SINs and allowing subscribers to see the evolving rep of any other subscriber. Before you choose to deal with someone, you can view their rep score. If it's negative, you can take your business elsewhere.

Other rep systems are more global in nature. Legal citizens can join up with **I-Sez**, a global community that links your online reputation, provided by individual ratings along with cumulative ratings from any social networks you belong to in a publicly accessible format. The system's goal is "creating an open society that rewards strong ethics, kindness, and metahuman connections." In addition to subscribers checking out other subscribers, parents check I-Sez or other similar networks to check out their kids' friends, employers use the system to check out potential (or current) employees, and schools check out prospective students.

For those of us who live in the shadows, ShadowSea has a beta-test rep system in place providing "credit ratings" to runners local to Seattle. Runners can get ratings from Johnsons, fixers, other runners, or anyone else in the shadow community. ShadowSea also links a "crime-o-meter" to their rep sheets, showing an amusing caricature of a thermometer to indicate a runner's "Wanted" status with authorities. Of course, ShadowSea's system is based on a handle, not a SIN or ID, so some runners with bad reps have tried to create new personas and start fresh. (Other runners frequently catch on to that trick, so I don't personally recommend it.) Johnsons and fixers can check out a runner's rep score before hiring. Runners can check out another runner before hiring them for a run, or check out the rep of a fixer before signing on.

Six months ago, ShadowSea added a "professionals" category where street docs and other "service providers" can be rated. ShadowSea bases the credit rating on real-time feedback and ratings, so if a runner screws up, his or her credit can take a dive as soon as the shadow-gossip hits ShadowSea. I've seen folks go from a sterling rep to bottomed out in a few seconds once their face got splashed up on the evening newsfeeds.

## MEDIA AND ENTERTAINMENT

» Ask most wageslaves what they use the Matrix for most, and entertainment is going to take the #2 spot (after work, of course). Heck, even I've been known to kick back with a glass of chardonnay and a good tear-jerker sim to while away an evening.
» Pistons

### POPULAR GLOBAL SOCIAL NETWORKS

**Consumables:** Purporting to affect corporate change through consumer decisions, promoting product safety, fair pricing, and corporate overwatch, their motto is: "Our nuyen, our lives, our opinions matter." This is a great place to get—and post—info on products, everything from chewing gum to grenades. If you want to check something out before you buy it, subscribe to this network.

**GAIANET:** An environmental watch group that posts everything from shamanistic earth-friendly blogs to runner-obtained video footage of corporate environmental abuse. It's a meeting place for back-to-nature hippies and environmental terrorists like Terra-First! While the network is mostly just talk they hit gold occasionally, like the recent exposure of Radisys Chemical that resulted in multiple arrests of Radisys executives for dumping toxins in Tacoma.

**Matchmakers:** The most popular of the dating services (or perhaps just the one with the largest subscriber base), this fee-for-service group allows members to post their details and their preferences for companionship. The network allows you to see if someone meeting your specifications is within range and even provides meeting suggestions. The network also provides a live blogging feature, advice columns, a rating system for everything from restaurants to florists, streaming video, and audio files on everything from personal grooming to pickup lines and their signature "Ten Best Places to Kiss" lists for major sprawls around the globe.

**GamersUnite!:** All things game-related are supported by this social network. It provides a meeting place for gamers of all kinds—AR, VR, even board games—and helps link up multi-user games with players. Members can rate games, discuss strategy, post cheats, and kibitz about their favorite games. This network is also the favorite dumping ground for software pirates, and users frequently can download copies of the latest and greatest (even unreleased) games that they've cracked.

**MagicNET:** The old standby got a new facelift after the Crash 2.0. Awakened users can meet and mingle with other likeminded folk, discuss the latest theories, and post spell formulae (including illegally obtained copyrighted formulae, if you know where to look). There's also special areas devoted to all the wacky paranormal things Mother Earth's been throwing at us.

The media and entertainment corps—frequently one and the same—have risen to meet the desire for never-ending newsfeeds, on-demand sims, and instant access to global information. Pay-for-service streaming newsfeeds provide commercial-free news, while the "free" services often are loaded with advertising spam. If you're looking for flashy, sensationalist news broadcasts, check out the


large media networks, like Ares' Truman Distribution Network or Horizon's Turner Hisato. If you want somewhat unbiased coverage, you'll want to look to the new crop of "citizen journalists" or personal blogs.

Underground news networks are a longtime tradition. With simple-to-use recording features standard on most commlinks coupled with massive blogging networks, the underground news network has shifted to an individualized perspective. Popular blogging networks like **Connections!** allow metahumanity to share its life stories—complete with video, texting, and subscriber feedback—with anyone who cares to see it. **MetaMatrix** is an Evo-owned social network that relies heavily on metahuman citizen-journalists, or CJs, to provide a meta point of view on issues that the mainstream media frequently ignores. Many of these networks have a huge global following, connecting citizen-journalists and/or attention freaks with subscribers around the world. Being a CJ is easy—all you need is a commlink with video and audio recording and something to record.

» It doesn't have to be something interesting, mind you. Connections! is loaded with so much amateur video junk that actually finding a useful story can be almost impossible, though the really hot stories tend to spread through the system like wildfire. They claim to be a "clean" network, but there's a constant upload of homemade porn for those eager to get up close and personal with a CJ's extracurricular activities.
» Snopes

» Blogs can be a great way to learn about a potential mark or figure out a corp's weakness. It is amazing what people will talk about. 'Course, most corps have pretty strict rules about blabbing on new projects or talking about your boss's foot fetish. They employ search agents and corporate hackers to search out the really incriminating blogs.
» Slamm-0!

» Pirate media outlets are another great place to get real news. These folks are cutthroat, frequently hiring runners to help scoop a story. If you want real, relevant, and gritty stories provided with a minimal amount of sensationalism or bullshit, check out a pirate network. **KSAF** is my favorite in the Seattle area.
» Sunshine

» That's a bit shameless, isn't it?
» Kat o' Nine Tales

### Gaming

Virtual gaming is a huge matrix entertainment venue. While online gaming was once the province of geeks locked in their parents' basements, nowadays AR has brought virtual gaming out of the basement and into public venues. Interactive AR games like *Electronic Ninjas* allow participants to challenge other gamers to duels when they encounter a nearby opponent, engaging them in an AR combat. The current top game is *Rocky Mountain Avatar*, which pits contestants against each other as T-Bird smugglers. The courses are based on real physical objects. Many malls and public areas sponsor their courses to improve foot traffic. Someone at the Bellevue Mall in Seattle, for example, would be notified when another gamer was in his or her vicinity. They could then challenge each other to run the course. You can frequently spot the hardcore gamers by their erratic—and often dangerous—movements and actions as they respond to an AR fantasy world disconnected from their physical surroundings.

VR games are even more popular, with many gaming corps producing almost-BTL level experiences even through cold-sim connections. Persistent rumors of programming illegal levels of biofeedback haunt the industry, with popular games such as *Glitterworld* being investigated. In VR, you can become anything you'd like, from the producer of a nova-hot sim to a medieval dragon slayer. Some games are prize-oriented, drawing millions of participants, spectators, and complete media coverage.

» If you prefer your gaming in a more personal social setting, gaming cafes and dens are hugely popular. Some are simply coffee shops taken over by gamers, while others actually provide areas, even "coffins," for gamers to rest in while immersed in VR.
» Kat o' Nine Tales

» Some sell BTLs and CalHots or run a bit of Matrix gambling on the side, or even provide customers with online porn. Not all of them. If you're looking for a fix, though, chances are you can find it in a gamers' den.
» Beaker

### Simsense

Simsense is wonderful technology that lets people step out of their own dreary and depressing lives and into another world.

While the cheaper commlinks are only AR enabled, fancier models allow users to connect to the Matrix via cold-sim—cold meaning that it isn't possible to fry your gray-matter through the signals. Hot-sim enabled 'links are illegal. Of course, riding a motorcycle without a helmet is illegal in most places too, and for similar reasons—no one wants to see bits of your brain smeared on the highway. But that doesn't stop too many people. These days, even cold sim is pretty damn mind-blowing. Recent advances in downloading BTL-quality hot sims via wireless technology has trickled down to seriously improve the quality of cold sim.

We embraced simsense as a society a few decades ago. Back then you could always tell you that were in a computer construct; "almost as good as the real thing" was the catchphrase. "Better than life" was reserved for highly addictive simchips that delivered ultra-real sensation while simultaneously frying your neural pathways. Now, however, the quality of simsense entertainment and gaming venues has enticed an entire generation into VR to experience the wonders of the electronic world. Virtual vacation sims allow a Seattle wageslave to experience a glowing blue ocean and brilliantly white Caribbean beaches without leaving their living room. Relaxation sims programmed with psychologically tailored mood music, colors, and scents are available. You can get drunk in a virtual bar, enjoy all the taste of a steak in a virtual steakhouse (without any of those pesky saturated fats), even meet up with a talented companion in a virtual brothel.

With so many great things to offer to the wageslave, is it any wonder that simsense is so popular? Instead of being Bill the Accountant, you can be One-Eyed Bill, feared pirate in a sim-seas VR game, or compete in *Glitterworld* along with millions of other entertainment hopefuls. While reality is limiting, simsense is freeing. An entire generation has become hooked.

• I remember being a kid and having my mom worry over how much time I spent with my computer. Now, no one thinks twice about someone who spends all day plugged in at the office, then comes home and plugs in for some virtual R&R. Oh, every now and then some public health flunky sends out a warning about the harmful effects of having such a sedentary society, or how kids' brains need sunshine to grow, or some other anti-wired bullshit. For the most part, it's so commonplace to live large parts of your life plugged in, enjoying some cold sim, that no one blinks at it.
• FastJack

• I saw some recent stats that Matrix-based addictions (excluding BTLs and the like) were now the most common addiction in UCAS, finally passing caffeine. Unlike caffeine, though, most Matrix addictions are psychological (rather than physically based).
• Butch

• If I could just get a caffeine-drip while I was hot simming it, life would be perfect.
• Snopes

### AR/VR Clubs

AR has also taken over the nightclub scene. Many of the hottest clubs offer different DJ track list subscriptions channeled directly to your commlink, allowing each guest—or connected group—to listen and dance to different tunes. Even in clubs with live performers, the act is enhanced with AR, including adding in multi-level sim feedback available through a 'link. For those of us who prefer there are a variety of VR clubs where you can socialize with others in the comfort of your customized iconic self. The best VR clubs and bars offer near-BTL-level experiences, so the Kamikaze drink you order can give you a realistic buzz (you can even wake up with a hangover, if you program your feedback right), and you can feel the silky soft skin of that pretty blue lady you're dancing with. Some clubs require patrons to have metahuman forms while others allow any icon you can imagine ... so you could be dancing with a storm cloud, having drinks with a large, featureless marshmallow, or arguing warez piracy with a neon dragon.

Private Message...

• Sugar, I got your note about the best clubs around. Here's a few of my favorites. I can get you a VIP pass for any of them, in return for an itty-bitty favor ... .

**PCP, Hong Kong**: A purely VR nightclub, with strict regulations on the icons allowed inside (metahuman shapes only), this place prides itself on original music from top-notch performers, with hit songs and scores that never see the actual light of day. The club's iconography changes based on the music playing, as do the drinks and eats available, and the rumors are that a team of technos does the decorating. A staff of wiz programmers are available to help guests modify their icons to fit into the theme, in case you show up dressed for heavy-metal and end up with swinging jazz.

**Ion Dreamz, LA**: A virtual strip club catering to any and all preferences, from the most mundane to things you probably haven't even imagined. There's a special area for swingers and folks who enjoy more hands-on entertainment, but you need to know who to ask (try Jerry, she's a waitress on the *Imaginarium* floor). A word of warning: the drinks at this place are hardcore, as the management has discovered that the more inebriated the client, the higher the tips.

**High Rollers**: This is a posh gambling network which attracts high rollers from around the globe. No idea where it's based at, since in most places this network is highly illegal. The imagery is amazing; if you want the feel of a flamboyant Las Vegas casino, or a quiet game of high-stakes poker, or anything else (including betting on—or participating in—actual blood sports), they've got a spot on the network for you. If you want to visit, there's a backdoor to the place at the Coliseum in Seattle ... least there was last time I checked.

**The Masquerade, (varies, but in Europe):** A virtual rendition of the Grand Tour, where the more tech-savvy of the high and mighty come to associate and hobnob in virtual splendor. Invitation only, *mon cher,* but if you can get in (through either an invitation or some very clever hacking), it's worth the visit. The setting is generally a lofty ballroom, with crystal chandeliers, solid gold floors, and gem-studded fixtures. There are quite a few secure "side-rooms" that branch off from the main ballroom, where the powerful can slip away to make backroom deals or find some virtual alone time.
• Kat o' Nine Tales

### Advertising/Spam

Of course, you can't mention the Matrix and media without discussing advertising ... or spam. Corporations love AR because it allows them to constantly throw advertisements at potential customers. Everyone's link is constantly tracking their spending patterns, sending purchasing—even just browsing—data back to parent corporations, who hoard the data like a dragon does gold. Pause by a window display of sporting equipment? Browse the site for a ski lodge in the PCC? Don't be surprised to have dozens of vacation offers, sales ads for outdoor sport equipment, promotional offers for winter clothing, and even multiple offers of "snow-bunny" hook-ups clogging up your commlink. By analyzing your buying patterns, your spending habits, and your shopping preferences, corporations can target you with specific ads designed to get you spending.

There is a fine line between advertising and spam, however. Everyone has their own definition of where this line is drawn—personally, I tend to drop an ID as soon as I get repeat ads for services, which takes anywhere from a few days to a couple of weeks. Once the line is crossed, all that virtual junk becomes spam. Spam filters are sold by every major 'link provider, software developer, and megacorp. The catch is that while they may temporarily filter out competitor's spam, they invariably allow their own affiliates' spam to get through. Singularity's **SafeShield** and Renraku's **SPAMOUT!** are popular, although SafeShield tends to shut your 'link down completely when it gets overwhelmed in a spam zone.

## SPRAWL MANAGEMENT

Cash strapped cities and governments privatized most essential sprawl management functions decades ago. The wireless Matrix is no different. Touting wireless Matrix as *the* future, promising easier administration and lower costs, private corporations led by NeoNET fought over lucrative government contracts to build and operate wireless infrastructures. Now, everything from waste management to law enforcement uses wireless technology to help manage daily life in the Sprawl.

Most cities also have several Matrix Service Providers, or MSPs. When you sign up with an MSP, you get a commlink number that's transferable if you ever switch providers. You can purchase a commlink and then activate it by choosing a MSP, or sign on with an MSP first and receive a "free" commlink with your contract. Most wageslaves use the free commlink, although it's frequently a lower-end model loaded with crapware. Also, many MSPs will only work with their brand (or affiliated brand) of commlink. For us runner types, there are also black MSPs, catering to those individuals who value privacy (and don't really want a background check run when they sign up).

**PSYCHOLOGY TODAY: ARG**

Augmented Reality Grief, or ARG, is the newest psychological catch-phrase for a variety of symptoms, such as uncontrollable anger, extreme violence, emotional outbursts, and unprovoked attacks on other online icons. Dubbed, "Road Rage of the Virtual Highway" it is a common occurrence, especially in heavy spam zones. [Link]

» To sign up with legal services or to buy a commlink, you need a valid SIN and ID, effectively shutting the SINless out of the wireless world.
» Fatima

» Unless, of course, you hack yourself and your chums an account.
» Glitch

» Or sign up with a Black MSP. In Seattle, the anarchist Left Bank hacker outfit runs one that's pretty reliable. If you know where to find their "office" you can get an account. You pay for the first 3 months service up front (and yes, their prices are high, and no, you don't get a free 'link), no questions asked, no answers given. When your cred clears, a commlink number is placed in a drop box. They provide anonymous message relays, temporary drop boxes, and a variety of other services—like pirated warez. Drop me a line and I can send you their way.
» Kat o' Nine Tales

» Fuchi Telecomm is another black MSP provider. Over the years, most of it has been divided up and hacked apart, but a section remains that was forgotten (no doubt through some fancy hacker-work) by all the major players. Its code was already deep inside the wireless Matrix infrastructure, and the antiquated accounts it sells work well on any NeoNET system, sort of piggybacking its way around.
» Glitch

## MATRIX CRIMES

» I've downloaded an excerpt from a cute little document that Lone Star provides to their new recruits during their "Wireless World, Wireless Crimes" class. Enjoy and feel free to comment.
» Glitch

**//Begin File Attachment//**

In the last 3 years, convictions for Matrix-related crimes (see appendix 7.41-B) has risen to 3 out of every 10 convictions. When convictions that contain minor Matrix charges in addition to other charges (such as using a commlink with pirated software while committing a more serious crime) are added, that number increases to 6 out of 10. Accordingly, it is imperative that you as Lone Star Officers have an understanding of common Matrix crimes and the criminals who perpetuate them.

**Common Matrix Crimes**

- Data theft from corporate facilities, including corporate espionage
- Copyright violations for software, multimedia, and entertainment downloads
- ID theft (compromising or using a victim's SIN and/or ID) and virtual robbery (stealing funds from a victim's bank account or charging purchases to an account)
- Fraud
- Privacy law violations
- Virtual vices (online gambling, prostitution, and exploitation*)

*Exploitation of minors often attracts significant media coverage, but prosecutable cases are rare. As Lone Star officers, you should be particularly sensitive to this issue.

» "Privacy Law violations?"
» Beaker

» Eavesdropping on wireless conversations, stalking, recording people without their permission in situations with the expectation of privacy. Which means I can take your picture at the mall, but I can't take it in the mall's bathroom—you can reasonably expect privacy while you piss. Basically being an annoying nuisance.
» Slamm-O!

### TOP 5 MATRIX CORPS TO WATCH IN 2071

**©Market Watch**

» I've added my own comments to each. And remember: "Behind every smart investor is a great hacker."
» Mr. Bonds

**1. Singularity: Matrix Corp of the Future**

Horizon's Matrix division handles the newest mega's online operations, provides online business services to a plethora of smaller corps, has a cutting edge software development department, and recently nabbed a multi-billion nuyen contract to provide educational software and online educational environments for the entire UCAS educational system. With that success, Singularity's stock is riding high. We expect great things from the charismatic Tam Reyes and his innovative staff.

» Singularity has a lot of technomancers on staff, and the software, hardware, and AR environments they've produced are nothing short of amazing (and almost impossible to reverse-engineer, making competitors *very* unhappy). I've also heard rumors that Reyes has some negotiations going to provide educational systems for a variety of other countries, which is a very profitable area that they're beginning to monopolize.
» Mr. Bonds

**2. NeoNET: Wireless Giant**

Any corp that puts a dragon in charge of its R&D gets our vote (here's hoping he doesn't mind the #2 spot!). The latest Matrixware coming out of NeoNET promises to keep pulling in the nuyen. In addition, as the pioneer, and continuing leader, in wireless infrastructure development, installation, and support, they're a sure deal.

» NeoNET was originally aligned with Horizon, but lately things have been tense between the two corps. Rumors are that Reyes has a personal grudge against the corp and is using some pretty dirty tactics to screw with them. A lot of runs have been targeting NeoNET's biotech branches. Make of it what you will.
» Mr. Bonds

**3. Xiao-Renraku Computer Systems: Safety Wiz**

Chances are, if you've bought security software or hardware for your link, you've purchased from Xiao-Renraku. The global leader in providing personal and corporate security for wireless systems, this corp has benefited immensely from the security scares of this last year. With recent polls showing that wireless safety was the #1 issue for consumers, expect Xiao-Renraku to continue to top the charts.

» Xiao-Renraku controls Hong Kong's Matrix grid together with Eastern Tiger and has successfully kept NeoNET out of the PacRim market. Seattle and Hong Kong both see a lot of shadow action resulting from that deadlock. According to some figures I "found," NeoNET has plans to ramp up their budget for their Seattle branch. I'm not sure that Xiao-Renraku's luck will hold out much longer.
» Mr. Bonds

**4. Mitushama Computer Technologies: Personal Computer Trendsetter**

Leading the pack in the production of popular commlinks and consumer electronics, this corp continues to win the race to sell consumers reliable, inexpensive tech. The highly anticipated MCTech Link 2071 is due to

***Continued on page 20***

Urgent Message...

## TOP 5 MATRIX CORPS TO WATCH IN 2071 *(CONT.)*

be released within the next 6 weeks and stock in MCT continues to rise based on sales projections.

» There's been some glitches in the MCTech Link 2071 that have pushed back the release date, but the reasons have been kept *very* well wrapped. My spidey-sense is telling me that the recent Horizon smear campaign on the safety issues of the MCTech Link 2070 has something to do with it.
» Mr. Bonds

**5. Kolkota Integrated Talent and Technology: Rising Star (or The Corp We Talk To Most)**

The service and consulting behemoth provides cost-efficient outsourcing for customer service, software development, and other tech-based services. Chances are, if you've called into a customer service hotline, you've spoken with a KITT agent, regardless of whether you were getting help with your Novatech Airwave or your Renraku Sensei 'link. In today's fully-automated world, their live sales and service support is winning them customers from around the globe. Their revenue tripled in each quarter of 2070, and projections for 2071 look to continue the phenomenal growth. Keep your eye on this rising star.

» KITT's been around for years, but they're really coming into their own as the ultimate outsourcing firm, providing everything from sales support to secretarial and HR services. Wages for KITTs primarily Indian employees are significantly lower than in many sprawls, and their level of education often exceeds what's available in most sprawls' workforce pools. With even the megas using KITT, there's plenty of opportunities for hackers to intercept the (mostly) administrative data that flows from their offices to their clients around the globe.
» Mr. Bonds

» Heh. That only counts if you're a hacker. Corps do it all the time. Well, maybe not photographing piss. But I bet they track your bathroom usage in order to market better TP to you.
» Snopes

» ID theft is a huge problem, but authorities aren't doing much about it. The law says you have to broadcast your SIN and ID in many public places—like malls—and that's just asking for trouble. The solution would be to allow folks to keep their SIN private, but then how could the corps track everyone? A hacker in a nice neighborhood is like a wolf in a hen house—easy pickings. With Joe Q. Public's SIN and ID, a hacker can go on a quick shopping spree.
» Glitch

» And if the hacker gets caught—and many of them do, greedy buggers—they can expect some serious jail time. Corporate jail time, if they "stole" corporate goods with Joe's money.
» Dr. Spin

» Consumers can buy services that monitor their SIN and ID and bank accounts for suspicious activity. ID insurance is also a big business—playing on fears of losing your ID. They promise to provide full ID coverage, generally by having DNA samples on file and counselors who help with the red-tape of reestablishing your SIN or ID in case of theft, loss, or computer glitch.
» Mr. Bonds

» Notice the mention of media coverage for "exploitation of minors"—the really disturbing crimes, often violent, like the creeps who peddle kiddie-porn or the pedophiles who attack kids online (or track them down in person). Those crimes happen daily, but the truth is, the creeps are rarely caught or even investigated unless the victim is a pampered corporate brat. Even when they are caught, if the crime was completely virtual (and with the sim-levels available today, you can bet those online attacks really do hurt and leave psychological scars), in a lot of places—Seattle, for example—the crime is generally just "contributing to the delinquency." This is one area where the law hasn't caught up to the tech.
» Frosty

» I've taken nuyen a couple of times—from parents generally, but once from a fed-up cop—to track down an "Opie"—Matrix slang for an online pedophile.
» Pistons

» You took money for that?
» Frosty

» To track 'em down? Sure. A girl's got to make a living, after all. But 'cause I'm so nice, I fried the Opie's brain for free.
» Pistons

An estimated 60-70% of Matrix crimes, when measured in terms of nuyen (for a cost basis, see appendix 2.11), are committed by crime syndicates (which includes organized crime, terrorist groups, and more sophisticated gangs). With the prevalence of wireless infrastructure, every major crime syndicate has come to rely on Matrix crimes for part of their money-making opportunities. Globally, our figures indicate—

**Load Appendix 5.16B...**

## SEATTLE MATRIX CRIME

In the Seattle area, the Mafia is responsible for the largest percentage of Matrix related crimes. Headed by Rowena O'Malley, they are suspected of money laundering, fraud, ID theft, ID forgery, operating illegal online casinos, BTL production, and distribution of illegal online pornography.

Of the Seattle Triads, the Eighty-Eights are the only Triad to have significant Matrix assets or dealings. We have reason to suspect that they recruit heavily among hackers and technomancers, which makes them more technology-friendly than the other Seattle Triads. They have a healthy business in software piracy and are believed to be one of the primary sources for illegal software in the city.

The Yakuza are suspected of using the Matrix to carry out "protection rackets" against virtual stores and businesses in their territory. They are also suspected of using hackers to hijack shipments or smuggle goods in and out of the city on container ships by altering online records and customs documentation.

Of the two remaining Seoulpa Rings in Seattle, the Choson Ring is almost entirely virtual; most of their crimes involve the Matrix in some form. They operate online casinos (some illegally), are suspected of regular data-thefts and online bank-robbery, and ID theft/forgery. In addition, they are suspected of using their gang connections to coordinate smuggling around the Pacific Rim, using hackers to forge shipping records.

**//End File Attachment//**

## WAREZ

On a related note, warez—pirated software or black-market programs—are big business in the crime world. Warez come in a variety of flavors—from the customized Exploit program specifically designed by and for hackers to legitimate programs that some enterprising hacker has liberated for personal use or resale. Warez can be bought through a major retailer, like Hacker House ('course, you're going to need to be a hacker to get into their sales node) or from local dealers.

Let's say you want Xiao-Renraku's newest search assistant, **Fetch.** Assuming you have a valid SIN, ID, and bank account, you could go to the virtual mall and pick up a copy for 129¥. Or you could look up your favorite warez dealer—maybe a hacker friend, a friendly Triad, or a local matrix gang—and buy a copy for 10¥. 'Course, you won't get all those nice corporate updates ... but what do you expect for 10¥? Software piracy costs corps billions of nuyen every year.

» Warez tend to be more prone to problems and glitches. Personally, I think the corps purposely build their software to be glitchy. Legally purchased software gets all the necessary updates. Pirated warez don't, and eventually all those bugs make them unusable. Who needs copyright protection when you know a hacker only gets a few weeks or months out of your prog before wanting to unload a couple of bullets into his 'link?
» Glitch

» Course, if you fiddle with the corp software yourself, you can also take out the all the crap they load into it–like "consumer tracking."
» Slamm-0!

» That kind of paranoia gets real expensive, real quick.
» Netcat

» So says the lady who doesn't need programs.
» Puck

» Puck, you ever heard the one about the pot and the kettle?
» Netcat

### COMMON SPRAWL USES OF WIRELESS TECH

- In Seattle, RFID tags in packaging materials enable Seattle's waste management contractor to monitor the level of recycling in every household, mechanically sort recyclables with greater efficiency, and levy stiff fees against households that discard recyclable materials improperly.
- Gridlink systems connect vehicles to vehicle registrations, calculate and automatically bill road-usage fees, monitor traffic, and use complex programs to reroute vehicles to manage rush-hour traffic.
- Intra-city air traffic systems connect with air-traffic, providing automatic air-traffic control, verifying licenses, monitoring illegal air traffic, dispatching drones, police, or automatically issuing citations, and cutting down on in-air collisions.
- Wireless police and public safety drones patrol neighborhoods and public areas, allowing police forces to cut down on personnel and costs. Drones can provide real-time footage of busy public places, monitoring for criminal activity, checking for valid SIN & IDs for metahumans where that data is required to be broadcast, analyzing and recording suspicious activities, and providing public assistance (giving directions, calling for medical attention, assisting with lost children, and other "good citizen" functions).
- City streets and buildings are kept clean by a fleet of service drones controlled by a city management contractor. In inclement weather, such as heavy snows or flooding, streets can be constantly maintained and kept drivable. Specialized drones with sensor equipment that can detect stress points in buildings, bridges, roads, or other public infrastructure, are sent out at regular intervals to analyze and provide limited repairs, or to notify city administration of potential building or infrastructure failure.
- Restricted access areas (such as high-class neighborhoods) or membership-only facilities ranging from sports gyms to country clubs use RFID tags in members and/or specialized encrypted broadcasts from members' commlinks to provide secure, unobtrusive access. In secured facilities such as daycares and schools, biometric scans may be required to verify the RFID tag data for adults accessing the area.
- Shopping centers and stores track RFID tags embedded within merchandise to automatically tally up purchases, charging customers' store accounts or bank accounts when the customer leaves the shopping area.
- Public transit systems track the number of broadcasting IDs waiting at each bus, train, subway, or lightrail stop to provide accurate analysis of ridership, enabling the public transit authority to dispatch more transportation to routes with heavy ridership loads or longer wait times and to constantly analyze the most efficient use of transit resources.



### Pirate and Hacker Crews

You can't talk about Matrix crime without talking about Matrix pirates and hacker crews. Pirate crews frequently violate copyright laws and hijack intellectual property. Chances are, if you've picked up one of those "free" copies of the latest "Nathan

Never" sims or used a multi-user access code for *Rocky Mountain Avatar* posted on a filesharing network, you've benefited from a pirate crew. Hacker crews are a bit more profit oriented and delve deeper into the realm of Matrix crimes—but we'll talk more about them later.


## DATA HAVENS

Knowledge is power, especially in the shadows. If you come across something interesting during a run—new drone design specs, psych records for a politician, even the itinerary of a popular goblin-rock star—someone out there is willing to pay good nuyen for it. The problem for most of us is that we don't know that person and we certainly don't trust them. Instead, you take the data directly to an info broker. He or she will pay you and then resell it. You can also purchase information from an info broker if you can meet his or her price. Info brokers provide a valuable service, for which they charge a hefty fee, and are some of the most well-connected people in the shadows.

Data havens work along the same lines. Some charge a fee to access data. As a runner, if I had some valuable data, I could upload it to the data haven. If someone wanted to see it, they'd pay a set fee. I'd get part of the fee and the data haven would get the remainder. Other data havens are maintained as free resources, such as the Nexus or the Helix. Some are even legal: the Library of Congress in UCAS, for example, (which holds a copy of every item written in the UCAS, digitally or otherwise). In fact, local governments often house public records in government data havens.

» Asgard is an orbiting satellite that holds one such data haven, although it more often resembles an online auction house. They specialize in really hot, really recent data—as in upload directly from corp X, do not stop, do not pass go. Great place to go if you've got something too hot to hold on to or are worried about getting a bullet before getting paid. When they get something, they post a summary of the data and open bidding on it. High bid wins the data. They don't shut anyone out of the bidding, so yes, that means that sometimes a corp will buy back its own secrets. Data that doesn't get purchased at auction often gets dumped into the data haven, which you can browse, but they charge for the browse and for any data accessed—which can get real spendy, real quick. Generally worth the nuyen, though, considering the timeliness of the data. Anything older than two weeks gets dumped back down to other data havens and is free for all.
» Orbital DK

» You also should know that Asgard's take of the auction is generally between 60–80% of the sale price. As far as I know, though, no hacker has ever been traced from Asgard. Perhaps the confidentiality is worth the price.
» FastJack

» The free data havens are just as useful. First thing a hacker should do is get him or herself an account at the Nexus, the Helix, ShadowSea ... hell, at every data haven you can find. Having good intel is the difference between surviving a run or dying a fool. You can find rumors on people, notes from runners on security holes they've seen at a hot research facility, up-to-date info on shifting gang alliances and territories ... you need it, you can find it.
» The Smiling Bandit

» The biggest problem with data havens, especially the free ones, is trying to sort through the outdated, random, or purposely misleading data to find the hidden gold. Most data havens have researchers, hackers who do nothing but eat and breathe the data in them. If you don't have the skills, browsing software, or time, I'd suggest paying a researcher to help you sift through the shit to find what you're looking for.
» Netcat

» Governments and corps hate the underground data havens, but they don't let that stop them from accessing the data, just like you and me. So remember, paranoia is healthy. Take everything with a grain of salt, yadda yadda.
» Glitch

Many of the data havens existing today are part of a shadow network, a loose agreement to provide data-sharing and backups among the network members. After the Crash took down Shadowland and many other data havens, sysops realized just how vulnerable they were.

» It was this loose affiliation that allowed Captain Chaos to distribute info on the worm to the other shadowlands around the globe, saving thousands of lives and years of accumulated data.
» FastJack

Most data havens already had been sending old and outdated data to the Nexus, the biggest data haven (before and after the Crash). As systems attempted to rebuild post-Crash, there was

a general agreement that in order to protect from another such attack, the shadowy data havens had to build a more reliable network. That's how the Shadow Network was formed, allowing member data havens to mirror each others content. Most havens also still send regular back-ups to the Nexus.

## MATRIX LAW AND POLICE

Matrix law is a tangled mess of conflicting laws, disparate punishments, and cross-jurisdictional nightmares. What else would you expect when your meat body can be squatting in the Seattle sprawl while your mind breaks multiple laws in Hong Kong? Different countries and corps have different ideas of what is illegal (frex, modified Browse programs that are perfectly legal in Salish-Sidhe territory are highly illegal in the PCC) and very different ideas of appropriate punishment. Add in the immense amount of corporate nuyen that flows along the Matrix and the possibility for our world-wide economy to get rocked if (or rather, when) something happens to said Matrix, and you end up with one thing: Corporate Court intervention.

The Corporate Court established the Corporate Court Matrix Authority (CCMA) years ago. After all, anything the corps get their hands into, the CC is required to meddle in too. The CCMA is meant to keep inter-corporate hi-jinks down to reasonable levels. They're responsible for Matrix regulations, including passing final judgment on issues such as universal wireless protocols and jurisdictional issues, making sure e-commerce continues to run profitably. That means stepping in when corps get too aggressive with their black ops, harassing wireless network providers who inhibit e-commerce with shoddy maintenance, frequent downtime, or shabby security, and intervening when the corps start squabbling on—or over—the Matrix.

The CCMA took a huge hit after the Crash in terms of personnel and reputation. Someone had to be blamed and the CCMA was a convenient scapegoat. After all, if they'd been doing their job, they would have known about Winternight and the worm before the crash. It didn't help that they'd lost most of their officers.

• That's total crap, blaming the CCMA for not preventing the Crash. Most of 'em were boot-licking bureaucrats who knew more about corp politics than writing script.
• Slamm-O!

In the years that have followed, the CCMA has been overhauled. They've embraced the wireless world and seriously pursue anyone who tries to hamper it. They care a lot less about doing the corporate dance and a lot more about policing the corps themselves. To do the policing, they rely on the Grid Overwatch Division.

### Grid Overwatch Division

We hackers cause so many problems with our ability to break multiple laws in multiple jurisdictions at the same time. With the appropriate use of agents—or sprites—a hacker can cause more havoc than any souped-up street sam, at least in terms of Matrix borders crossed and laws broken. On a single run, you can illegally hack access to a Seattle MSP provider, hack a NeoNET sat network, access a KITT HR data storage, and break into a Horizon R&D facility. If the Horizon corporate security hackers try to trace you, they'll have to hack through NeoNET's sat system, too. Which is rather the same as sending armed Horizon goons onto NeoNET's property. In other words, it ain't gonna be pretty.

To make matters worse, many jurisdictions have completely different laws regarding Matrix crimes. Hacking in Caracas isn't much of a crime at all. So unless a corp can send their own goons after you, requests for local assistance are going to get laughed at.

In an attempt to help regulate Matrix law, the CCMA created the Grid Overwatch Division, cleverly nicknamed GOD. Staffed with corporate security hackers on loan from each of the Big 10, they are responsible for policing the tangled mess of the wireless Matrix. They track down hackers and solve cross-jurisdictional crimes when corporations need someone to help referee an investigation. If necessary, they'll investigate crimes on their own, especially when corporate black-ops are heating up a little too much. The G-men, as they're called, are primarily confined to public nodes. However, when investigating a crime, they'll ask for permission to cross onto private space. If permission isn't forthcoming, they can get warrants that'll allow them to enter. The Big-10 all make a show out of helping out the G-men, citing the standard line of "Matrix crime hurts us all."

The reality is that under the surface, cooperation is frequently limited or delayed, especially when you combine the godlike attitudes of the G-men and the rather strict enforcement of the CCMA. That, combined with the fact that corps use runners to hit their competitors, and their need for time to make sure there's no evidence linking them to those "deniable assets" means that the G-men can find their investigations hampered.

Don't let that lull you into a false sense of security. The G-men are good. Recruited from the top corporate security hackers and given free rein and rather unlimited power, there is a reason they call themselves GOD. They carry the most cutting edge programs, have the best gear, and huge egos—mostly earned.

• GOD lost a lot of G-men during the crash. Most of them went down trying to fight the worm, others ended up in comas or with severe AIPS. They're back to full strength now, though.
• Pistons

The G-men have standardized icons, with brimmed hats, trench coats, badge, and Tommy gun iconography. Most also keep a few other icons on tap for when they need to browse through a data haven or scope out a hacker-bar without getting evicted (or mobbed).

Frequently, the G-men like to patrol public nodes, looking for hackers, trying to spot them through their falsified IDs or catch them as they start hacking. Once they spot someone suspicious, they'll run a trace while they distract the hacker—often with a bit of online combat. G-men aren't just combat hackers, though. They're excellent detectives, used to tracking down criminals and solving politically sensitive crimes.

• There's a lot of rivalry and show-boating between G-men from different corporations. They all want to make their corp look good and the others look bad. They've been known to go to extreme lengths to solve crimes and show up the other G-men.
• Glitch

» Yeah, that's on the backburner right now after the "discipline" of a Renraku G-man. She ripped thru an Evo node without a warrant, fried two Evo sec. hackers, and crashed the node—which happened to be running an intensive-care medical facility. The CCMA came down *hard* on GOD. The G-men have been watching their step ever since, but rumors are they're only acting polite. Corp rivalries are even worse now that they can't let all those aggressive, ego-ridden tempers out to play.
» Pistons

» GOD has been trying really hard to recruit technomancers. Problem is, the corps that have 'em don't want to loan them out. The few that have joined up with GOD (outside the special-forces Artificial Resource Management, or ARM, division) have faced prejudice, razing, and harassment from the other G-men, to the point of violence. Two technos from Horizon walked off the job recently and apparently Horizon is making some noise about it. Expect to see more shakeups at GOD, or at least a big internal smack-down as the technos from ARM attempt to teach the other G-men some manners.
» Netcat

» GOD also has a Transmissions Fraud Division, investigating scams transmitted over public wireless systems. Generally they only get involved when the victims are from multiple corporations (or multiple MSPs complain to GOD). If scam artists target non-corporate citizens, then the regular security firms—like Lone Star or even national police—investigate. Because of this, most scams are targeted to non-corp citizens.
» Mr. Bonds

» Yeah, but some of those wage-slaves are just so damn trusting that it's hard to resist ... all that disposable income, and they'll believe *anything*.
» Snopes

» GOD has a special ops force that doesn't appear on "paper" anywhere, so to speak. I've heard them referred to as the RH—I'm guessing it stands for Right Hand (keeping with GOD's tradition in naming their divisions). Tasked with hunting down terrorist groups who might target the Matrix, these guys make the regular G-men look like script-kiddies. Ruthless, lethal, and not at all inclined to rely on the legal system to deal with suspected terrorist groups. Too many organizations wanted to "keep watching" Winternight instead of taking action. The RH was created to make sure another Crash never happens, and they've got carte blanche to deal with problems the way they see fit.
» Fianchetto

» The RH has worked with Horizon's Dawkin's Group in a few cases. Apparently the two groups have a tenuous working relationship.
» Dr. Spin

### Other Law Enforcement Agencies

If you do something big enough to interrupt commerce, expect the G-men to come knocking. For everything else, there's your local law enforcement—corporate, government, or contracted. Corporations investigate Matrix crimes that affect their bottom line, like software piracy, ID theft, or hackers that use or target corporate assets. Some governments have their own law enforcement—like the PCC, with their nationalized law enforcement and their very intolerant views on hackers. Most other jurisdictions rely on contracted law enforcement, such as Lone Star.

Lone Star's Matrix Crimes Division, MCD, is tasked with patrolling public Matrix spaces and providing rapid response, investigation, and incarceration of Matrix criminals for areas they're contracted to protect. The overworked Lone Star detectives have to deal with everything from Matrix gangs running BTLs to reining in organized crime. In between, they get stuck trying to police hackers, ID thieves, warez dealers, and all the other riff-raff that make a living off the Matrix. Lone Star also will provide Matrix security to customers, including IC and on-call combat hackers.

Like any service-corp, Lone Star balances their actions based on profitability and customer satisfaction. That means that if hacker has been making the news, they'll devote much more resources to catch him than on busting the kid who is selling pirated sims at school. If it'll make them look good, they'll make it a priority. After all, satisfied customers tend to renew contracts, and if you impress customers, you can charge them higher prices.

» The moral is: if you keep a low profile, they've got too many other cases and too few detectives to hunt you down. If you make noise, botch a run and kill a few bystanders, or start dumping malicious code that fries kids' brains, you'll get moved to the top of the pile. They've got the resources to hunt you down—it really is almost impossible to disappear in today's surveillance society, so do yourself a favor and don't give 'em a reason to move you to the top of the "to-do" list.
» Glitch

## PANOPTICON: ARE THEY WATCHING?

A few centuries ago, some brainy guy had the bright idea to build prisons that would police themselves. How? By making it possible for the security guards to watch all the prisoners, all the time. His idea was that if the prisoners *thought* they were being watched, they'd behave, regardless of if there was anyone watching or not. Good thing they didn't have micro-drones and mini-cameras available, eh?

Well, looks like his idea has finally come to life. And not just in prisons—actually, that was pretty much a bust, since criminal types tend *not* to care if they're being watched in jail—after all, they're *already* in jail, so what else can happen? It's the *honest* citizens, the wageslaves and corporate sheep, who happily plod along believing that some good shepherd is watching over them. Most don't think twice about the requirement to broadcast their SIN and ID in public places. The ubiquitous drones whirring by are ignored, just part of the landscape. It's assumed that cameras are watching everywhere, omnipresent. No one thinks about the data trail they leave every time they access a public ARO, buy a soy-kaf, ride a bus, or enter a public or private area. Before the worldwide wireless Matrix initiative, it was possible *not* to leave a data trail. Heck, it wasn't even that difficult; using credsticks, anonymous bank accounts with the Malaysian Independent Bank or some other private institution, a commcode number registered through a black-market service ... all that and a nice suit, and you could pretty much go anywhere without raising flags.

Now, to operate in the sprawl, you have to have a SIN, an ID, and a commlink. Everywhere you go, every icon, storefront or public terminal you access creates a record. Drones patrol the street, scanning people to ensure they have commlinks broadcasting the right data. Cameras are imbedded everywhere, recording and analyzing every move. Wireless transmissions are intercepted, analyzed, and recorded. Or so we've been told. So we believe.

Is it true? Are "they" really watching, all the time, everywhere, everyone? Well ... yes and no. Psychologically, it doesn't really matter—if people believe they're under surveillance, they'll act accordingly. In corporate areas, like office buildings and the like, there probably is someone watching. In public spaces, there isn't enough man-power or funding to really staff all those surveillance systems, so they rely on programs and agents, which aren't particularly great at operating outside their programmed parameters. Now, if they're looking for someone specific, then they can track them down. If a crime does happen, they've got it recorded. Lucky you.

• I'd like to point out that numerous studies have shown that this theory *doesn't* work, that omnipresent camera surveillance has done little to nothing to decrease crime, and that the only thing it *has* done is helped destroy civil liberties and give authorities unlimited opportunities for abuse.
• Aufheben

## RFID TAGS

These tiny guys are so ubiquitous that most people can't remember back a decade, when they were reserved for corporate logistics and tracking valuable employees. Now, almost everything comes with them—anything you buy with packaging, that's for sure. Clothing, toys, furniture, even that candy bar you bought this afternoon from the vending machine. The RFID tags contain data and can broadcast it up to 40 meters, perfect for short range messages or inventory control. Most people don't bother to disable the little tags, so as they walk around the street, they give off dozens of little bits of information about themselves, from their underwear to the chewing gum in their purse. Corporations use this data in conjunction with your ID to better market things specifically to you.

• Runners disable the little buggers so we don't have to deal with underwear sales ads intruding on our meets with Mr. J. and his friends. Tag erasers are cheap. Buy one. Use it. Often.
• Glitch

• RFID tags can be placed in anything. Yes, anything. That includes the gooey bar you ate for lunch and the soy-kaf you guzzled down. You are what you eat ... .
• Netcat

• If having your lunch broadcast its presence from inside your tummy bothers you, you can choose to eat some of Horizon's Naturally Yours organic food line. They guarantee no artificial ingredients—including RFID tags—are added.
• Traveler Jones

Corporations frequently place RFID tags inside their employees. With a RFID tag broadcasting, you can track any of your employees within a secured compound. You can make sure only authorized employees enter sensitive areas, you can see who employees are eating lunch with and even time how long they spend in the bathroom. If the tag is biomonitor-enabled, you can also keep track of your employees' vital statistics—which is very useful for security personnel as well as personnel working in dangerous conditions, like mining or biochemical research labs. Most corps write RFID tags into an employment contract. (Where they insert the tag is up to the corp.) Many corporations also offer free RFID tagging at birth for employee children, promising peace-of-mind to new parents and a convenient way to keep track of all their future little wageslaves. Biomedical ID Tags are also popular with parents and caretakers of the elderly—they contain medical data, including allergies or medical conditions, along with broadcasting basic bio-monitoring and ID data.

If you lose a child, the local police can put out a KIDAlert, which notifies all public and private nodes of the child's RFID tag data. Anyone subscribing to the KIDNetwork will be able to scan nearby tags to see if they can spot the child's data (the first private citizen who scans the kid's ID is paid a 1,000¥ reward). The recovery rate is over 90% for children tagged and registered on the KIDNetwork (and less than 30% for those not on the system), and the KIDN aggressively markets those statistics to parents. Elder care programs often utilize these tags as well, since if an older person suffers a medical problem away from caretakers, responding medical personnel can access their medical data—including insurance info—immediately. DocWagon and other medical service providers offer free tags to all their clients.

The broad coverage of wireless towers in most sprawls enable easy GPS positioning. That means, boys and girls, that if you've got

a tag on you and you're within range of a wireless tower or relay point, you can be physically tracked. Your commlink isn't the only thing broadcasting a signal, a fact you'd do well to remember. And while law enforcement and public services may maintain that GPS system, hackers have just as many reasons to use it.

» If you plan an extraction, you better have a tag eraser with you. Be sure to watch out for stealth tags, which are almost impossible to spot. Damn little buggers.
» Mika

» Law enforcement uses RFID tags to keep track of criminals. Sex offenders get tagged (generally someplace not so easily removed); if they go within a certain distance of a school or childcare facility, their parole officer is notified and a warrant can be issued. There's been fighting in courts over placing RFID tags in sex offenders that broadcast their crime, so that anyone who comes within range is notified that they are a SEX OFFENDER. Ruins their lives, since who wants to have that in their building, workplace, or, well, anywhere? Occasionally one of them will end up beaten or dead at the hands of vigilantes. So far, UCAS has held that it's legal. It's up at the Supreme Court later this year; we'll see if they uphold it.
» Kay St. Irregular

» Gee, it's a good thing that everything a RFID tag broadcasts is the truth.
» Snopes

» Another trick for law enforcement (or the corps) is to spray out a RFID tag "mist" that blankets a crowd with microscopic tags, enabling them to track protestors, rioters, vandals, etc. even after the fact. Some corps use this as a passive measure to track criminals who break into a facility.
» Hard Exit

» If you're tracking someone—maybe for an extraction, maybe you want to keep track of a suspicious Mr. J, or just want to bug your ex—you can slip a tag onto (or into) them, then tap into the system. Doesn't let you watch 'em or listen in on them—you need spy gear for that shit—but it will tell you where they go.
» Mika

## SURVEILLANCE SOCIETY

If you want to live in the civilized world these days, you have to accept that surveillance is simply part of the package. Still, there are a few ways to get around the all-seeing eye. The most effective is to just make like a tree and leave. Go live in the Barrens somewhere or the middle of the Amazonian jungle (although I hear Horizon's working on bringing a wireless net there, too, so the birdies and beasties can make long-distance commcalls). There are countries that opt out of the surveillance web. Asamando, perhaps, if you can stand the smell. Trans-Polar Aleut, if you don't mind the snow and the lack of neighbors. If you want to live some place where there is paying work, though, you'll have to put up with the corps' invasion of your privacy.

Of course, if you don't have a SIN (by choice or circumstance), you'll be forced to survive in the edges of society anyway, like the Redmond Barrens in the Seattle sprawl or San Bernardino in LA. Without a SIN, you can't have a bank account, can't purchase a commlink, can't hold a job, can't even ride the bus into the welfare office—not that it matters, since you can't get welfare anyway. On the bright side, the gov't and corps don't know or care about your existence. Even better, you won't have to deal with spam.

Another way to avoid trouble is to realize that while the Man may always be watching, he probably isn't always paying attention. Be smart. Buy a fake SIN. Make sure it matches up with you—even the dumbest cop is going to know that a troll doesn't come packaged as a dwarf. Invest in some fake licenses for that 'ware and the weapons you can't leave at home, and try not to shoot people at bus stops. Have a couple of extra IDs and the disguises to match 'em. Savvy runners utilize alt-skin, nano-paste, and latex masks to make sure their real face never gets seen when they're out committing crimes. Living a double life is a pain in the ass, but it's less than what you'd get doing twenty-to-life at a Lone Star facility.

» Buying fake SINs only works if you've got the money. At about 1,000¥ for the cheapest (which won't do much more than let you ride the bus as a police scan will pop it as a fake almost immediately), it's out of reach for most of the SINless in the barrens. People who want to get out often have to hock their souls to a fake-ID outfit, like the Mafia or a Matrix gang. Or, if you're the right age, you can hook up with the military. A bunch of UCAS recruiting stations have moved to the edges of the barrens—used to be kids came to them. Now, those kids can't even walk across town, so the military has come to them. For a lot of the kids, it's the only shot they'll have of getting out of the Barrens, or even seeing their 20th birthday.
» Fatima

On the bright side, if you're trying to run surveillance on a mark or just stalking an ex, really good hackers can tap into the surveillance system and use it for their own purpose. Just like using a GPS system to track someone, if you can tap into, say, Lone Star's street camera system, you can monitor your mark as he cluelessly goes about his business. Tap into the GridLink system and you can monitor that box truck carrying some valuable gear you'd like to acquire. The possibilities are endless.

## DATA SEARCHES

Anyone can run a data search. Pop a name and SIN into the search box and click go. Even the clumsiest user can perform a search on something—or someone—that will return amazing amounts of information. A basic search on a person can turn up name, birthdate, birthplace, parent's names, employer, work history, criminal history, education, marriages, even a SIN. In-depth searches can turn up even more. And that's just by a regular Joe; hackers and technomancers can dig up information that even the subject didn't know. The only way to ensure your privacy is to step off the grid, and become SINless. For most people, though (runners excluded), that is too high a price to pay.

Data searches are just a fact of life for wage-slaves. Schools run them, employers run them, the government runs them. Runners like us may have a slightly different view, depending on if you started out with or without a SIN. If you have a real SIN (even if you don't use it), you'll be in the system. Smart runners will want to erase data relating to themselves. SIN deletion is costly, time consuming, and so intricate that only major syndicates and hacker crews have the

capabilities and resources to do it right. It's a big job—going in and getting rid of cold-storage backups, checking into every consumer database and deleting the records, deleting medical files (including those hardcopy backups and storage of DNA samples), education records, criminal records … . The organizations that offer "ID deletion" services charge a high fee, and it's worth every penny.

If you don't have a SIN, the police may be able to run a search on you, but they'll come up blank, or with a fake SIN if you've used one (or even worse, with multiple fake SINs if you haven't been careful to have those erased). It all depends on what criteria they're using to search and what biometric data is linked to your SIN(s), real or not. If they don't find anything with a search—'cause you've been careful up to now—that doesn't mean they won't start compiling data. Leave a hair or some skin cells at a job site and your DNA will be in a database somewhere, even if it just labeled "unknown." Eventually, if you keep running, chances are they'll catch up to one ID or another and all those "unknown" bits of data will finally have a name to attach to them.

• I highly recommend everyone run periodic searches on their own name and ID(s). If you can't hack into Interpol's Criminal Database, get a hacker buddy to do it so you can see how close they are to really tracking you down. With all the cold-storage backups, it can be a pain to get data "erased," but it is possible. It's easier the earlier you catch it, though, really.
• Glitch

• I'd highly suggest having your fake IDs erased by a professional crew. Many of the syndicates and crews that create fake IDs will also thoroughly erase those IDs that have gotten too "hot" to continue using. If you don't, the cops will eventually start linking all those fake IDs to you, especially if they have biometric or forensic data linked to them. Accumulated data like that is bad.
• Fianchetto

• You can expect to pay more, likely double or triple the normal rates, if you want a crew to delete an ID that has forensic or biometric data linked to it that's stored at a police facility or is being used in a current investigation.
• Haze

• This is why having a hacker as a friend is just so damn nice. We do things like data searches and erase incriminating bits and bytes before they come back to bite (or before they get downloaded into cold storage).
• Pistons

• As a note, the "Hey, baby, want me to erase your life?" line is a bit creepy. You might want to try something new.
• Turbo Bunny

• But that's not what you said last week. ;>
• Slamm-0!

### PRIVACY: AN URBAN LEGEND

Ok, so with all the surveillance, biomonitoring RFID tags, and easily available data on your panty size, you'd think privacy is a thing of the past, right? Not really. Privacy is real for those folks at either extreme of the socio-economic bell curve. The SINless have privacy because they just don't exist. For the rich, privacy is a commodity that can be bought and sold. With enough money and influence, you can remain above all that corporate data-raking: keeping your purchases private, ensuring that your education is from institutions that don't share student data, patronizing only those medical facilities that promise the utmost discretion and back up those promises with a hell of a lot of IC.

For the rest of the world, the average wageslave, privacy is a very valuable illusion. Privacy laws are highly touted as protecting citizens. The average citizen believes the data out there about himself is there for his own good—medical records available for doctors and medical facilities to share, ensuring his medical conditions will be known regardless of where he is, his personal information makes it easier to find potential dates, make shopping easy, and keeps the neighborhood safe from gangers and criminals. In his mind, his privacy hasn't been invaded. And in this self-obsessed, blogging, and virtual exhibitionist society, a large percentage of the data available actually comes from the wageslave himself.

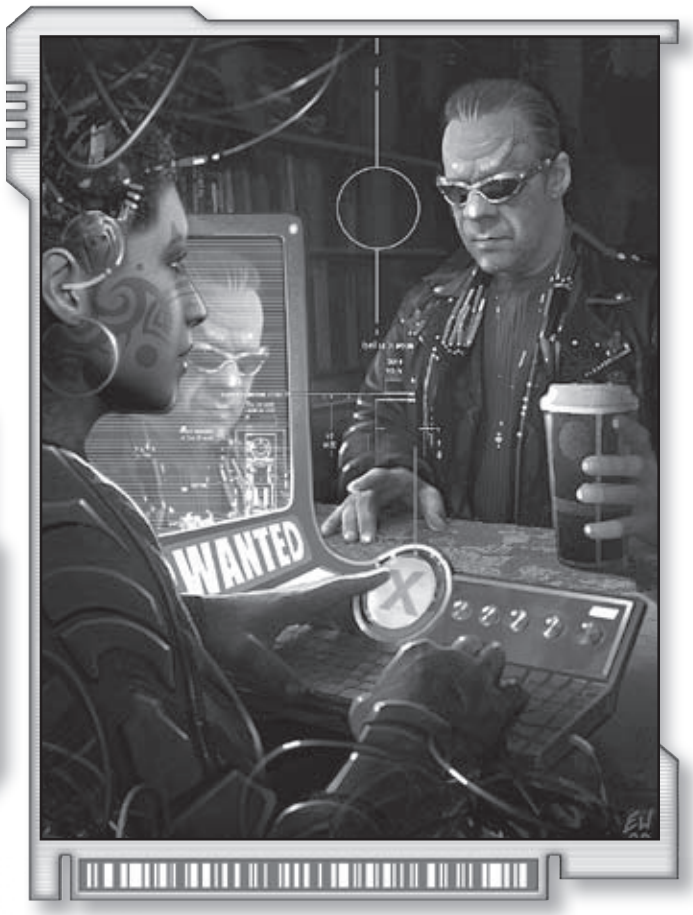
### SOUSVEILLANCE: WHO WILL WATCH THE WATCHERS?

As obsessed with video-diaries, blogging, and citizen-journalists as folks are, it shouldn't be surprising that sousveillance is as popular as it is. Watching other people is almost as fun as posting information about themselves. For some, this is just another trendy way to connect with a social network or watch the world through another person's point of view. By joining a Sous-MoSoSo, like the **Diaries,** network members are outfitted with a constant recording device (generally hooked up via an internal camera in cybereyes or a camera imbedded within AR glasses or goggles) that records everything (24/7/365) the wearer sees. It allows watchers to become voyeurs—not of a specific person, but of the people around them. You aren't living their life or feeling their emotions, just seeing the world through another set of eyes.

Other people use sousveillance to make a statement, to try to police those who normally provide policing (like corporations, governments, and other authority figures) and try to enforce some level of honesty in an otherwise dishonest world. By recording the actions of police, for example, they hope to bring accountability to the officers who believe they're above the law. It's a nice theory and it works on occasion—and can provide some very nice blackmail material—but corporate powers tend to blackout negative press. Sousveillance networks have sprung up to counter that, combining with social networks to bring breaking news to millions of people at once before a corporation or government can stop the flow of information. Of course, that's why corps have their corp spin departments … .

## SHRINKING GLOBAL VILLAGE

The wireless Matrix has shrunk our world. The concept of *distant* is no longer relevant to people connected by a simple thought in the virtual world. For many, the virtual world is as real as anything outside of it. "Neighbors" means who's closest to you on your social network, not who's down the hall in your apartment building. Breaking news in Hong Kong can cause panic or fear




in Seattle (like we saw last year with the technomancer hysteria). Your favorite virtual store could be based down the street or on a different continent, but your purchase arrives just the same. Your employer could have an office building and a thirty minute commute, or, just as likely, you could log on to a virtual office where your boss is based in England, your secretary in Kolkota, and your favorite "coffee break" buddy is in NYC. A college professor could be based in LA and be lecturing to kids in Madrid.

Ask most people in Seattle how far away Neo-Tokyo is, and they'll shrug and reply, "about 3 seconds." Most commlinks come with an automatic time-zone adjuster, which lets you know the time of the place you're calling, just in case you forget that the sun doesn't rise in Neo-Tokyo at the same time as in Portland. For many people, that small digital time display blinking at the uppermost corner of their commcall is the only reminder they have that their best friend lives an ocean away.

That means that people become concerned about things that would never before have touched them. The media's constant broadcast of global news brings home even remote threats, if they're sensational enough. The Seattle ork slasher murders has orks in cities across the globe jumping at shadows, as if the murderer will fly across oceans to skulk in their alleyways. The recent disappearance of twenty children in New Orleans has parents across the globe flocking to the KIDNetwork to protect their own offspring. A tense terrorist standoff in London will have viewers tuned into the streaming newsfeeds 24/7, hanging on the real-time developments. Public interest is held by the shocking and the scandalous, not necessarily the relevant.

The interconnectedness that the Matrix allows also provides like-minded individuals the ability to connect in ways unimaginable a few decades ago. Patients suffering from extremely rare diseases can connect virtually and exchange advice and commiseration. Chess competitions can draw players from around the globe. Conservationists interested in the fate of the three-toed sloth can meet for virtual conferences and organize virtual sit-in campaigns to raise awareness among local officials.

## RELIGION

Religious and spiritual organizations—those that don't condemn it out of hand—use the Matrix to bring congregations together. Muslims around the globe can subscribe to MeccaNET, joining a global community, having the ability to attend virtual (or AR) services in a Mosque, and synchronizing their clocks to the prayer times in Mecca itself. Catholics, attempting to revive a flagging interest in their religion, have embraced the advantages of wireless technology, broadcasting live AR feeds from the Vatican, allowing AR confessions and absolutions, even providing entirely virtual masses. Other religions have declared the Matrix anathema, but those religions are finding that their members have a hard time dealing with the modern world.

» And many of those radical religions have a tendency to show up on corporate watchlists as potential terrorists. The thought being that you are either for or against ... no middle ground.
» Fianchetto

» Some groups have actually managed to avoid being upgraded to the wireless world without being labeled terrorists. Quakers in UCAS are one group, bunch of farmers that live like they're in the 19th century still. Actually ride *horses*, if you can believe it, and grow their own food. They've got a special exemption from the UCAS gov't to live outside the rules.
» Mika

» At the opposite end of the spectrum are new religions—or cults—like the Virtual Purists. They believe that the Matrix is the next step in human development, a realm where they can shed the limitations and temptations of their flesh and live a purely spiritual life. Adherents attempt to live in a purely VR state. Some even commit suicide while in VR, hoping to shed their mortal coil. Becoming purely

**SEASOURCE SEARCH:**
Sousveillance

*The recording and scrutiny of authority figures by those under their authority, particularly those who are the subject of surveillance. Also, the recording of data from metahuman point-of-view at metahuman eye-level.*
Do you want to watch *sousveillance* videos? [Link]
Do you want to enter a *sousveillance* Chat Room? [Link]
Do you want to post your own *sousveillance* video? [Link]
Do you want to join a *sousveillance* forum, social network, or mobile social network? [Link]

Urgent Message...

### POPULAR SOUSVEILLANCE VIDEOS

**Knight Errant Attacks SINless Man**—Watch three uniformed officers approach a sleeping ork and kick, punch, and taser the man. *See official KE response that man was "resisting arrest."* [Link]

**Students Face Racial Discrimination at Harvard**—Watch as the dean of admissions culls out ork applicants, instructs admissions counselors to "encourage the tuskers" to apply to a state university. [Link]

**Humanis Policlub Members, Revealed**—Catch the action as a group of HP torch a local troll family's home, then return to their homes and *unmask*. Hear police response. [Link]

digital, apparently, means they've achieved a purely spiritual form. Free from the flesh's lust, anger, hunger, thirst, craving for material goods ... well, you get the point. The Virtual Purists are gaining popularity, too, led by a very charismatic person named Reverend Illias. The "transitioning" is accompanied by elaborate ceremonies, attended by other "initiates" of the religion. Reverend Illias attends each transitioning virtually, welcoming the newest member into the fold. I've heard—mind you, just heard—that if the person fades away with his body's death, it means he didn't have a pure enough soul, or perhaps didn't have enough faith, or just wasn't ready to transition to the next level of human spirituality. Unfortunately for the VPs, most jurisdictions consider an attended suicide the same thing as murder, regardless of if the person claims to be "transitioning" into a digital form. That's put Reverend Illias on the most-wanted lists of a few governments and organizations, like Horizon's Dawkin's Group.

» Goat-Foot

» Is it even possible to live just in the Matrix? I've heard the Ghost-in-the-Machine stories like everyone else. Aren't they just urban legends?

» Ethernaut

» Weeellll ... I certainly wouldn't recommend swallowing cyanide and then jacking in to see what happens. But I think a lot of us who spend significant time in the Matrix have seen things we can't explain.

» The Smiling Bandit

## THE NEW LANGUAGE

The availability of real-time translation programs, of universal iconography, and of developing iconographic languages has eroded the language barrier that used to stand between us. If you're speaking to someone via an AR or VR connection, you can use an interpretation program to assist your communication. Free services, like Babel-Tree, are fairly handy and universally known, although there are translation delays between when you speak (into the program) and it translates into the chosen language. Babel-Tree relies on continual customer feedback and input, so it supposedly manages to keep up with current slang and provides fairly accurate translations that catch real meaning, not just syntax. Corporations often use professional grade programs or even high-level agents to provide translation services for complicated subjects, like conferences between research scientists, where the slightest misconstrued word can ruin an entire project.

Most public newsfeeds are broadcast in a variety of languages, regardless of their country of origin. Music, sim, and entertainment downloads can be customized into almost any available language (if there's demand for that language, that is). With the proliferation of teaching sims, many people learn multiple spoken languages. Even in-person interactions can be made easier by the ability to utilize real-time translation and prompting software or services. Babel-Tree has a very popular searchable database filled with examples of phrases, words, and slang spoken by native speakers. If you're at a meeting and want to be polite, you can have Babel-Tree running; mentally say a phrase and the search returns the same phrase, translated, for you to repeat.

Written language is another issue altogether. So much knowledge can be converted into an auditory, pictorial, or iconographic media that being able to read is no longer a necessity. In fact, instead of focusing on increasing literacy, the focus has shifted to creating a standardized iconographic language. A new form of communication, relying on symbols, pictures, sounds, and cobbled together words has become the Matrix version of city-speak, a bastardized language born online. It's easy to pick up, very intuitive, and is very fluid—instead of being standardized, it relies on the constant evolution of human-Matrix interactions. Even someone with no exposure to Matrixese can pick up essential messages in the language with little or no prompting. Horizon has been a major push behind this new global language, and AR ads in Matrixese are popular among the younger population.

## TRANSPARENT POLITICAL PROCESSES

Another global impact of the Matrix is how transparent the political process has become. Politicians can target ads directly, speaking through AR to targeted audiences, holding virtual rallies, and conducting real-time polls to gauge their popularity. Many governments have instituted public broadcasting for public interests, allowing citizens to see what is going on in the "hallowed halls" and provide live feed-back to their representatives. Corruption charges have raised in the popularity of sousveillance of political figures and offices. Somehow, knowing their constituents are watching supposedly keeps the politicians honest. Most politicians also allow constituents to link directly into a "voters-network," with posted polls and areas for feedback.

In the UCAS, over 90 percent of the Senators in congress have a live-feed access for their constituents. When a new proposal or bill comes up for a vote, the text of the bill is posted online along with a more concise summary. Interested voters can read (or listen to) the bill and send their opinion (generally a yea/nay vote—occasionally small messages are allowed) directly to their Senator. The system allows constituents to see a measure of the for/against responses, as well as the percent of the population who've responded. When the Senator votes, he or she can make decisions based off of what the people really want, rather than special interest groups hired to influence the Senator.

» And if 80% of voters wanted a "yes" vote and their Senator votes "no," it generally makes some major news, at least in DC. Senators

who cater to special interest groups have to really watch their toes now, because too many votes against their constituencies' wishes means they won't get re-elected. Or worse yet, the scandal will get them shunned by the rest of Congress ... and the special interest group nuyen will all dry up.
• Kay St. Irregular

Voting, at least in the UCAS, is done via encrypted transmissions of an individual's votes within a voting "window"—generally a week long period that the virtual voting booths are open. Other governments that rely on a voting system follow similar structures, although the time required to transmit and count the votes varies. Generally speaking, though, to register to vote you need a SIN and a certified electronic address. Some governments, more security conscious than the UCAS, send voters a biometrically keyed encrypted ballot. It requires that the voter provide biometric verification, such as a thumb print or retinal scan in order to fill it out. In the UCAS, the system is pretty much that each ballot is provided with an encryption system for when it is returned via the wireless Matrix. Voters are required to sign electronically that they did, in fact, fill out the ballot themselves. How's that for trust?

• And remember, in the UCAS, it's One SIN, One Vote. That means if you buy multiple SINs, you get multiple votes. Now go out there and do your civic duty.
• Snopes

• It seems like it'd be easy to rig an election just by hacking voters' commlinks, or intercepting the wireless transmissions, decrypting them, and editing the votes as you'd like. However, the system actually works pretty well (for that part, at least). Since every citizen sends their votes in individually during a week-long voting window, the votes come trickling in during the entire Election Week. To make a measurable difference in the results, you'd have to hack tens of thousands of commlinks (hoping they hadn't already mailed the vote) or attempt to intercept the transmissions—easy for maybe a handful, but hard to coordinate large scale. If you want to screw with elections, you have to do it at the vote-tally office and ever since the California Magestone debacle, UCAS keeps their voting results ICier than Antarctica. It'd be possible to screw with a minor election, or even a major one with enough nuyen and backing, but it'd be easier—and cheaper—to just hire a PR firm like Charisma Associates to convince folks to vote the way you want.
• Kay St. Irregular

## HACKERS, RIGGERS, AND SPIDERS

With the world's reliance on the Matrix, people who can manipulate it are a corp's worst nightmare and biggest asset. To a corporation, having someone who can protect their data while stealing their competitors' gives them the advantage. To the average citizen, hackers and riggers are mostly known through sims and newsfeeds. An employee probably only interacts with someone at an outsourced helpdesk, never actually meeting the security hackers that work for his company unless he screws up. Likewise for corporations that employ spiders, riggers who hook into a building or campus and "wear" it like a second skin. Most employees probably don't even realize they're in a spider-controlled facility. Runners better know, 'cause that's the kind of ignorance that'll get you killed.

In the media, hackers are portrayed as either scummy identity thieves who rob innocent bystanders to feed their drug habit or brainy, socially inept members of a runner team—the teammate that solves complex puzzles but can't speak coherently in front of the opposite sex. There's little of the romanticism that you see with mages, more's the pity. And even more unfortunately, the wildly popular EpSin-Team trid show has cast-type riggers such as Jerry Drone, the surly dwarf with a creepy spider-like drone always clinging to his shoulder, a man who can hot-wire a tank or crash a 747 with a few wild waves of his short arms.

• Well, there's public opinion and there's fact. Hackers today need to be more than just brains. You can't hide in a basement and do overwatch anymore. IC or a bad biofeedback filter used to be the worst thing a hacker came up against. Now, a hacker who doesn't know how to handle themselves in a fight—or at least how to duck—isn't going to last through the first run.
• Glitch

But the public spotlight certainly isn't on hackers and riggers anymore. With the unveiling of technomancers, AIs, and sprites, suddenly hackers don't seem quite so threatening or interesting. Combine that upstaging with the fact that hackers have taken a lot of the heat directed towards technos, and there's been a large upswing in the amount of animosity between the two groups.

The threat of technomancers has led to a new crackdown on hackers and an increase in the punishment for electronic crimes. Hackers have been mistaken as technomancers and given radical

drug treatments during incarceration to prevent them from "unleashing their powers." Unfortunately, this has led to cases of drug-addiction, serious brain damage, and even death. While the rest of the world is slowly learning to accept the new powers in their midst, in the shadows, the conflict between hackers and technos is escalating.

» Upswing? Escalating? Seems like the "animosity" started out high and hasn't budged.
» Netcat

» Yeah, well, we all do the same job, only you technos think you can do it faster and without expensive programs or gear, just the help of your little sprite friends. Most of you are also off-your-rocker crazy. It's hackers who get the blame when the heat drops, and I'm supposed to get all buddy-buddy with you freaks? I don't think so.
» Clockwork

» 'Cat, you know that's not how all of us feel. I've worked with you in the past and I'll be happy to work with you again. From your rep score, it looks like most of us here on JackPoint feel the same.
» Pistons

» Hey, even I apologized. Clockwork is in the minority here.
» Slamm-0!

» That's just 'cause you wanna see 'Cat naked.
» Kat o' Nine Tales

» *roll eyes*
» Netcat

## TECHNOMANCERS AND AIS

Since the big Queen Elizabeth hospital scandal and riots in Hong Kong last June, the world has been terrified of technomancers. The Tlaloc situation cooled things down a bit for the technos, as everyone tried to duck and cover from an AI in a hijacked space station with some biowarfare weapons aimed down at us. Then, of course, *everyone* was introduced to Pulsar, the charismatic AI all buddy-buddy with Horizon. Pulsar saved the day with Tlaloc, becoming a global hero and a golden poster-boy for the AI movement. Two years ago, no one was talking about technomancers (even those of us normally in the know) or AIs. Now, you can't turn on the trid without seeing Pulsar or one of his Undernet AIs on a late-night talk show, hearing about the latest techno theory, or getting sucked into one of LA's newest Matrix reality shows. Pulsar and Horizon's major media blitz accomplished what they'd hoped: AIs are predominately seen as benign or even friendly (according to polls).

I'm not going to get into all the facts and figures right now. I'm just going to touch a bit on what's been going on since things cooled down in 2071. First of all, most countries have passed resolutions forcing technomancers to register, much like mages and shamans must. Since it appears that actually recognizing technomancers can be a bit difficult, the registration systems are fairly reliant on the honor system—for now, at least. As more technomancers join ranks with security organizations, perhaps we'll see technos scanning passengers at airports or sniffing each other out in crowds, just like wage-mages do today. For the moment, it is possible to hide techno abilities from the authorities, much to their chagrin.

Legally, the issue of AIs has been fairly convoluted. Horizon was the first corporation to declare AIs to be fully sentient beings, eligible for full corporate citizenship. It even handed out SINs to the AIs that sought refuge with the corporation. The courtrooms have been full from that action, since other corporations cried foul. However, many other nations have followed suit, most notably the PCC and Tir Tairngire, providing AIs with citizenship in return for certain promises.

### NEWSNET LIVE FEED, HOSTED BY HOLLY HASKINS ...

Final arguments in Xiao-Renraku vs. Horizon, the century's biggest court case, were presented yesterday. Today, in just seconds, the world's highest court authority, the Corporate Court, will make a final ruling in the case that has caught the world's attention. Xiao-Renraku claimed that Horizon has stolen their copyrighted data and has asked the Corporate Court to intervene. Horizon, however, claimed that they've simply employed a sentient being, capable of making such decisions, and offered it full rights as a Horizon citizen.

The being in question is Teskit, an AI. At stake: the future of all AIs who've sought citizenship and equal rights with corporations and governments around the world. All eyes are watching as the court hands down its decision. The court bailiff is reviewing the decision. The decision is being announced ... and ... *Teskit is a sentient being with the legal right to choose his own country or employer*! What an amazing victory after such a long fight!

Now let's look at public opinion from around the city, captured as people celebrated—or protested—the ruling! Here's what a few people had to say:

- *Pam V., waitress*: Of course I'm on Teskit's side. It's slavery, that's what. I don't care where he lives, out here or online, no one has the right to enslave him.
- *Oscar M., EMT:* Look, the thing is, it doesn't have a pulse. It wasn't born. It can't even survive if there's a power failure. The programming code came from Xiao. Plain as the nose on my face, it's a Xiao program. What's next? Free the toasters?
- *Sandy P., student:* I think it's cute. Those big brown eyes, y'know. You can see it's terrified of going back to Xiao. And who blames it? They just want to pull it apart to see what makes it tick, y'know? It may not be "alive" but it can think and feel. That's enough for me.
- *Rev. Les T., clergy*: God's grace has given us, mankind, souls. Mankind cannot in turn create creatures and breathe a soul into their being. The Pope has said that a creature of the Matrix is unable to receive God's grace; they cannot die and have no souls to ascend to Heaven. And without a soul, it cannot possess the free will that gives us the right to choose our own destiny.

# . . . THE MATRIX USER . . .

The woman in the black business suit passed a plastic folder full of paper across the table. "The dossiers for the team, coaches, and support staff, as well as their playbook. It's all there."

Chrome flashed as Ajax's cyberarm passed the folder to the freckled teenage elf sitting to his left.

"Hardcopy?!" the girl said incredulously, "Ew!"

Ajax's eyes rolled as his client took another disapproving look at the young hacker. "Mr. Ajax," she said plainly, "I really do have my doubts as to the composition of your team. While I have been assured that you have demonstrated past competence, your employment of minors in this situation lacks the level of professionalism that ..."

"Professionalism?" squeaked the elf, "You want professional, lady? Let me tell you some stuff, and then you can judge our professionalism.

"When we're done here, I'm going to spend half the time it takes to scan this hardcopy shit to evaluate the weakest areas of the stadium for electronic and social attacks. Then I'm going to build some back doors while my professional omae infiltrate the team and its families using credentials that I'll build while I'm pretending to be a normal kid at school tomorrow. I'm going to arrange the delivery of a box that I'll be using to get past the stadium's jammers and wireless blockers. I'm going to sleaze past both teams' hackers during the second quarter and slide a virus that I will customize myself into both teams' tacnet software. Then I'm going to feed information from the media and referee drones to both teams, and tweak the data streams so that the other team gets good intel. While that's happening, Yorick and Chordae and Lume will be deployed in the stadium posing as team staff members and doing their wicked little things to kill Seattle's chances this year. Then, after the game, I'll erase all evidence of our presence and provide overwatch to my team as we make our departure."

"Just a—"

"But you're right. If I was really professional, I'd have checked out our employer, too. I'd have sussed out her name by now, along with her position and maybe even her gambling history. If I was *really, really* professional, I'd have discovered that gambling on a fixed game is just a convenient cover for a twisted but ingenious ploy to arrange for a certain free agent to leave Seattle at the end of the season and take another team's offer."

The woman stared at the smug little elf, who shrugged. "If I was really, really, really professional, I would have already obliterated the data trail that could lead someone else to the same conclusion, as a professional courtesy to the valued client," she turned to Ajax, "I guess I'll get to work, boss."

Ajax smiled at the woman, "If she wasn't good, be assured we'd have dumped her freckled ass months ago. Shall we finalize the terms of our arrangement?"

The girl stalked off. "Fuckin' hardcopy ..."

While almost everyone who lives in a civilized area is a Matrix user in the Sixth World, the shadowrunning Matrix-specialist is a breed apart. Whether hacker, rigger, or technomancer, the Matrix-based character is the cowboy of the new wireless frontier. The tips, tricks, and new resources in this chapter will help players build their own hacking genius.

## CREATING THE MATRIX-BASED CHARACTER

The essential part of any Matrix user is their ability to connect. The commlink, sim module, and associated software are the primary tools needed to use the Matrix for most characters. This means that Matrix users can also serve other roles, such as magician or muscle.

Matrix specialists, on the other hand, make up a smaller proportion of shadowrunners. They are the digital wizards that get the team through security, bureaucracy, and even social entanglements. The term, "hacker," worries the average citizen and strikes fear into the heart of every corporate or government entity that has something to hide.

If people fear the hacker, they live in terror of the technomancer. If anything, the paranoia against these Matrix users is heightened by their unnatural ability to use the Matrix without any of the technological crutches of normal users. This panic over technomancers is not unfounded. The technomancer can reach unparalleled power in the Matrix, beyond even what technology can offer, although at a price sometimes paid in blood.

Something to remember is that most people use the Matrix, but not on the fundamental level that the Matrix specialist understands it. These are the people who can see inside the black box and make it their own. There are many diverse resources and tools that make up a good Matrix-based character.

### METATYPE

The Matrix is the great equalizer, a virtual space where people can look, sound, feel, and even smell like whatever they want. When the meat is left behind, it matters very little what metatype it is wrapped in.

Some metatypes offer advantages in different aspects the Matrix. The extra Edge of humans give that much of an advantage over the Edge-less agents and IC of various nodes. An elf's Charisma bonus is useful in social engineering, when one needs to interact with an actual person. The higher Mental attributes granted by the elf and dwarf metatypes are useful for technomancers. The extra Willpower of the dwarf metatype is a boon when dealing with the dangerous feedback of VR hacking and rigging. Similarly, while the additional Body attribute of ork and troll characters do not directly help resist feedback damage, the additional boxes on the Condition Monitor can be useful.

### ATTRIBUTES

Technology has created computer interfaces that allow the user to move through the Matrix at the speed of thought. However, being made of optical chips and electromagnetic waves, the Matrix moves at the speed of light. The body and the brain are slower than even the lowliest program, and as such a hacker's attributes are less important than his software and hardware.

Some attributes are important for Matrix-related tasks. Logic is vital when writing programs, hacking hardware (such as locks and other devices), and building or modifying drones. Willpower is extremely useful when dealing with feedback and dumpshock, two situations that all too often affect the Matrix specialist.

Technomancers, on the other hand, live and die in the Matrix by their Mental attributes. Willpower is probably the most important, doing double duty as Firewall against attacks and as part of resistance to Fading. Charisma also increases a technomancer's longevity in the Matrix, providing a bio-feedback filter against black IC, dumpshock, and rigging feedback. Response, and therefore Intuition, is not as important to the technomancer as it is to digital devices, but is still important in cybercombat, decryption, and reality filtering. Similarly, Logic sets the technomancer's System, which aside from providing defense against Matrix damage and greater connectivity is not as important to the living persona as it is to a digital device.

Resonance, on the other hand, is vital to the technomancer. Almost everything a technomancer does in the Matrix is influenced by her Resonance attribute, from maximum Complex Form ratings to Matrix attribute caps to Fading Resistance Tests. Resonance should be the first and last attribute the technomancer player should consider when building a new character.

### SKILLS

The Matrix constantly challenges the high-end user and his knowledge and abilities. A hacker's skills are as important as his hardware and software, dividing the elite from the newbie. The primary skills of the Matrix specialist are in the Cracking and Electronics skill groups. Players who are new to *Shadowrun* or to Matrix-centered characters should start by purchasing these skill groups.

The Computer and Data Search skills are the workhorses of the Electronics skill group. The Computer skill is especially vital for its use in Matrix Perception Tests (p. 228, *SR4A*); in a world where a rubber duck can be a file, a program, a gateway to another node, or even another hacker, the ability to analyze one's surroundings could mean the difference between life and death. Only slightly less important is the Data Search skill, as the hacker is almost always called upon to do the digital legwork and background research during runs. A hacker can do her job without using the Software or Hardware skills, but since the Matrix specialist is often also the technician of the team, these skills are good to have on hand. Technomancers, on the other hand, should consider the Software skill, as much of their power in the Matrix is in Threading.

The Cracking skill group contains the mainstays of the hacker. The foremost of these is Hacking: almost every way a Matrix user can misbehave is driven by the Hacking skill. In fact, the Hacking skill cannot be emphasized enough. Hacking is the most important skill for a hacker.

Electronic Warfare and Cybercombat round out the Cracking skill group. These skills mostly support the Hacking skill. Electronic Warfare is necessary for finding nodes and cutting through jamming, which allows the hacker to use Hacking. Cybercombat is useful for those times when the use of the Hacking skill would be too slow or fails and the hacker is forced to resort to brute force.

The technomancer must also consider the skills in the Tasking skill group. These skills are used to create sprites, which technomancers can use to great effect within the Matrix. Compiling is the most important of the skills in the skill group. Registering is close behind, allowing the technomancer access to the resources

of more than one sprite at a time. While the chances of facing an opposing technomancer are, in the early 2070s, fairly small, the Decompiling skill should not be overlooked as the threat of wild sprites and other strange phenomena grow in the digital realm.

Finally, the skills of the Influence skill group should not be overlooked. The only part of a person that is apparent in the Matrix is their personality. The ability to communicate in the Matrix is useful, if not vital to a team's success. Credentials can be created, paperwork planted, and authority authored, but such forgeries carry much more weight when presented by someone with confidence. Social engineering is sometimes a necessary part of the hacker's arsenal.

For non-specialists, the Computer and Data Search skills should be sufficient for life with the Matrix 2.0. Many of the actions that such characters perform are Extended Tests, so low skill ratings are still effective with smaller dice pools.

## QUALITIES

A character can be a Matrix user without taking a single quality. However, some qualities make a character more effective in the digital realm, and others should be avoided. In order to be a technomancer, on the other hand, a character must have the Technomancer positive quality or one of the technomancer qualities that appear later in this chapter (see p. 36). Some qualities to consider are listed below.

### Aptitude and Codeslinger

The Aptitude and Codeslinger qualities add to the character's ability to use one skill or Matrix action, respectively. Each may only be taken for a single skill or Matrix action, but if taken together and in relation, they can create a peerless hacker. For example, a character with Aptitude (Cybercombat) and Codeslinger (Attack) would be a fearsome force in the Matrix, while a character with Aptitude (Electronic Warfare) and Codeslinger (Detect Hidden Node) would know all of the secrets around her.

### Exceptional Attribute and Natural Hardening

Both of these qualities increase the longevity of a hacker. Natural Hardening helps protect the character against dumpshock and the feedback from black IC and rigging. An exceptional Willpower also helps against this damage, and aids the technomancer even further by increasing his Firewall.

### Photographic Memory

This quality may be overlooked by the average player. While file transfer rates are ridiculously fast in the digital realm, security is just as swift. Sometimes a hacker does not have the time to transfer a file or search for data. This quality allows the hacker to remember what she otherwise might miss due to a rapid retreat. This quality can also be used as "poor man's storage" for technomancers, who otherwise lack storage space.

### Adept

While magic and technology rarely mix, adept powers (see pp. 195–197, *SR4A,* and pp. 174–180, *Street Magic*) can readily augment a hacker's duties. Trodes allow a user to access VR without the invasiveness of cyberware, allowing an adept to keep her Magic rating intact. The Improved Ability power increases a hacking adept's skills directly. Improved Reflexes allows an adept to use her AR interface more quickly and efficiently, allowing her to approach the performance of VR while mitigating the risks. Eidetic Sense Memory can more reliably offer the same advantages as Photographic Memory, and Multi-Tasking makes a hacker more efficient. The Sustenance power allows a hacker to pull all-night coding sessions.

### Addiction

While this negative quality is not necessarily one a player would take at character generation, it is one that most hackers develop. Hot-sim offers several advantages to the Matrix specialist, but it can be as addictive as BTL simsense. A hacker using hot-sim on every run, without careful moderation, will slip down the slope to severe addiction and Essence loss. Technomancers do not need to worry about addiction to hot-sim, but have their own related problems (see *Technomancers,* p 129).

### Combat Paralysis

This negative quality is popular among players of Matrix specialists. Care must be taken, however, because this quality is triggered by Matrix combat as well as physical combat. When a node launches black IC, a character with Combat Paralysis will certainly have a lower Initiative than the IC and risks getting stuck.

### Technomancer

While this positive quality is obviously necessary to the technomancer character, it should not be taken lightly. Technomancers literally live in two worlds at once. It shapes their perceptions and their personalities, and they experience things that no non-technomancer could imagine. For more on what it is like to be a technomancer, see *Technomancers,* p. 129.

## GEAR

There are no two ways about it: a hacker is only as good as his gear. A good hacker needs a state-of-the-art commlink and bleeding-edge programs to tear up the 'Trix and master the digital realm. Even technomancers can benefit from the right equipment. The gear listed here can be found in *SR4A*, *Augmentation,* and *Arsenal.*

### Commlinks and Other Electronics

Every hacker has a commlink. While there are larger and more capable machines, the commlink can go everywhere the hacker needs to go, whether it be into secure corporate facilities or the battlefields of the Desert Wars. It is important for all of a commlink's Matrix attributes to be as high as the hacker can afford, although it is usually safe to skimp on Signal. A sim module is also vital when accessing VR, and the advantages of hot-sim modification should not be ignored. A simrig can also be useful for collecting intel on VR runs.

Characters might also find having an extra, weaker commlink advantageous. Such a commlink could be used as a "public" commlink, set to Active mode when in high-security zones while the real commlink remains in Hidden mode and acting as a combination of decoy and camouflage. Even technomancers may find such a commlink to be useful.

The Matrix specialist must also consider electronic warfare. A jammer, HERF gun, or EMP grenade (see p. 57, *Arsenal*) can be used to deny electronic assets such as drones or communications to opposing forces in the field. Defensively, the electronic warrior should consider a satellite uplink for its high Signal Rrating, and hardening to defend against electromagnetic attacks. Additionally,

a non-linear junction detector can find hidden electronics, and a chameleon suit can be useful when it becomes necessary to get close to low-Signal devices and networks.

Just about any item can be manufactured to include storage memory, from umbrellas to undergarments. Normally, this is incidental to the Matrix specialist, who uses plenty of electronic devices that already have plenty of storage space, but it is of particular interest to technomancers, who have no storage of their own.

### Cyberware

The Matrix specialist does not need cyberware to succeed, but it can give her an edge. One obvious item of cyberware for the Matrix specialist is the commlink, either integrated into a cyberlimb, cybertorso, or cyberskull, or implanted independently as headware. The largest advantage is that such a commlink cannot be removed without surgery. However, it makes it more difficult for the hacker to remain inconspicuous in a world of scanners and astral observers. The hacker cannot remove his implanted commlink (except as part of a modular cyberlimb).

Another important piece of cyberware is the datajack. This offers the user secure datajack-to-datajackwired communications with equipment and other people with datajacks by linking to them with a fiberoptic cable. It also includes its own memory, and an adapter that allows the user to access datachips directly.

If the hacker chooses to follow the cybernetic path and can afford it, she should look into a few other items of cyberware. An encephalon or simsense booster can make the difference when running against tough security. A control rig is necessary for riggers, but the hacker should also consider the option for collecting reconnaissance data first-hand with drones.

### Drones

While drones are the lifeblood of riggers, other Matrix specialists can benefit from having a drone or two. Mini- and microdrones can be carried in pockets or pouches, to be deployed at a moment's notice. They can be used for recon or to use as wireless bridges against systems with low Signal ratings. With the inclusion of spoof chips, drones can be used with less risk of being tracked. Additionally, an emotitoy (p. 57, *Arsenal*) can be used in social hacking situations.

### Programs and Complex Forms

The Matrix is vast and powerful, but a user cannot be a user without the proper tools. It is impossible to perform any Matrix action without the right program or Complex Form. Some are more useful than others. In this section, the discussion of programs also applies to Complex Forms.

Analyze is easily the most versatile program available to the Matrix user, specialist or no. It is used to detect hidden icons, evaluate Matrix constructs, and even defend against intrusion. It is a digital window to a digital world, and it should be a basic part of every Matrix user's load-out.

There are a few other vital programs that should be part of every hacker's repertoire. What Analyze offers the user in the Matrix, Scan offers in the physical world; a hacker cannot hack into a node if he cannot find it. Browse is another vital program, as the Matrix specialist will be called upon to do research before each mission. Stealth acts as a first line of defense against enemy icons.

These programs are enough for the "ninja" style hacker who infiltrates and escapes quietly, but some Matrix users are more comfortable taking systems head-on. These hackers use Attack and the various black IC programs to crash programs and trash enemy icons and spiders. They also have good Armor and Bio-Feedback Filter programs, so they can take as much as they can serve.

Programs can also offer advantages with social engineering. Sensor software such as Empathy and Lie Detection can be helpful when pretexting, and Facial Recognition can identify good targets in a crowd (see p. 60, *Arsenal*).

Non-specialist Matrix users should have Analyze running at all times, for their own electronic security. They should also have at their disposal Edit, Browse, and Encrypt, to facilitate normal Matrix use and safe communications with teammates.

## NEW MATRIX QUALITIES

This section describes new Matrix-related qualities for *Shadowrun* characters. For more details about qualities, see p. 81, *SR4A*.

### POSITIVE QUALITIES

The following are positive qualities, with a cost listed in Build Points (BP).

#### Chatty

**Cost:** 10 BP

The character is especially comfortable behind the mask of anonymity offered by the Matrix. The extra confidence grants the character a +2 dice pool modifier to Social Skill Tests when communicating via AR or VR.

### Intuitive Hacking
**Cost:** 5 BP

A character with this quality is highly intuitive about a single aspect of the Matrix. The character may perform one specific type of Matrix action without a program or Complex Form. The specific Matrix action is chosen when this quality is taken. For example, a hacker with Intuitive Hacking (Detect Hidden Node) may perform that action in the Matrix without a Scan program, adding only the Electronic Warfare skill to the dice pool. This quality may be taken more than once, each time with a different Matrix action.

### Latent Technomancer
**Cost:** 5 BP

A character with this quality starts the game as a normal, mundane character. When she starts the game, this character has no Resonance attribute or related skills, and may not spend BP on them. This quality may not be taken with any quality that confers a Magic or Resonance attribute.

At some point during play, usually some time after the start of the campaign, the gamemaster determines that the character's technomancer abilities manifest. This decision is entirely up to the gamemaster, and should not be discussed with the player. The gamemaster is encouraged to make the decision based on dramatic license and a good story. Often the ability will manifest itself in spurts, possibly leading the character to believe she is hallucinating or going mad. Often, a budding technomancer will unconsciously use her abilities before realizing that she has them.

Once the gamemaster had decided that the character's abilities have fully manifested, the character gains a Resonance attribute of 1. If the character has an Essence of less than 6 at this point, she still receives the Resonance attribute, although her maximum Resonance is reduced accordingly. If her Essence has dropped below 1, then she has no chance of ever being a technomancer.

When the ability manifests, the gamemaster also chooses three Complex Forms that the character gains for free at Rating 1. The gamemaster may also allow the player to choose additional qualities appropriate to a technomancer, such as Paragon or Synthetic Sympathy, but the character is then required to pay a Karma cost of twice the BP value of these qualities. The gamemaster also chooses a stream for the character that is appropriate to her beliefs and experiences.

Once the character becomes a full technomancer, she may improve her Resonance and learn and improve Resonance skills and Complex Forms normally.

### More than Metahuman
**Cost:** 5 BP

When jumped into a drone, vehicle, or rigged device, the character is completely comfortable, as though he had always had a machine body. When jumping into or out of a drone, vehicle, or rigged device, the character does so as a Free Action.

### Obscure
**Cost:** 5 BP

By a coincidence of bland statistics, average characteristics, and dumb luck, the data left by the character's life tends to get erased or lost in the enormous quantities of similar data in the Matrix. Any Data Search Test involving information about the character is made at a –2 dice pool modifier.

### Paragon
**Cost:** 5 BP

This quality is available only to those with the Technomancer quality. The character has made contact with a mysterious and powerful Matrix entity, which acts as a guide and grants certain advantages and disadvantages, see Paragons, p. 149. A character may only have one Paragon.

### Resonance Bond
**Cost:** Sprite's Edge x 5 BP

A character with this quality has established a resonance bond (see p. 160) with a free sprite that uses elements of its Resonance to augment the character's Matrix actions. The specific nature of the bond should be discussed with the gamemaster and is subject to his approval; see p. 160 for some possibilities.

### Synthetic Sympathy
**Cost:** 10 BP

A character with Synthetic Sympathy has an instinct for the cognitive processes of artificial intelligences of all kinds. The character gains a +2 dice pool modifier for all Social Skill Tests with AIs.

## NEGATIVE QUALITIES

By taking the following Negative qualities, the character gains the Build Points listed for each.

### AIPS
**Bonus:** 5 BP/level

The character has Artificially Induced Psychotropic Schizophrenia Syndrome, a psychological disorder most common to survivors of the Matrix Crash of 2064. For each level of this quality taken (max. 3), the character suffers a –1 dice pool penalty to Perception Tests while within Signal range of a Matrix device (including her own). Additionally, the gamemaster may require a successful Willpower Success Test with a threshold equal to the level of this quality when the character must focus her attention in a non-stressful situation.

### Data Shadow
**Bonus: 5 BP/level**

The character has a prominent feature, history, style, name, or other piece of information that makes him easy to locate in the Matrix. Any Data Search Test involving information about the character is made at a +2 dice pool modifier for each level of this quality (max. 3). Additionally, the threshold for any Track Test is reduced by one per level of this quality.

### Media Junkie
**Bonus: 5–30 BP**

This obsession with news, information, videos, forums, and social networking sites is a form of the Addiction quality (p. 93, *SR4A*), and acts as a mental addiction. It requires that the character have Matrix access, either via commlink or by virtue of being a technomancer. The BP bonus of this quality is dependent on its severity:

**Mild (5 BP):** At this level, the obsession seems more like a hobby. The character spends about two hours a day on the Matrix browsing through various public nodes and sites, but can skip a day without adverse effect. She also suffers a –2 dice pool penalty to Willpower Tests to resist the urge to surf the Matrix and to Addiction Tests.

**Moderate (10 BP):** The character has an obvious Matrix habit. If she does not spend at least four hours a day surfing the Matrix, she obsesses about her Matrix friends and the trivia she is missing, suffering a –1 dice pool penalty to tests involving Mental attributes, Resonance, or Magic. She takes a –4 dice pool penalty to Addiction Tests and to resist subscribing to her favorite nodes.

**Severe (20 BP):** At this level, the character clearly has a problem. She needs to spend at least eight hours a day browsing the Matrix, and she is fixated on the fan fiction, viral videos, email threads, and other trivia in which she is involved. Without her fix, she suffers a –2 dice pool penalty on tests involving Mental attributes, Resonance, or Magic. She also suffers a –6 dice pool modifier to Addiction Tests and to keep from logging on to her "My Favorites."

**Burnout (30 BP):** The character lives in a daze of Matrix sites and AR windows. She spends almost all of her time cycling through sites, constantly refreshing them to see if anything new has been posted. She sleeps very little and misses meals. Her Essence is reduced by one. If she fails to kick the habit, her Essence or one of her Mental attributes (gamemaster's option) will be reduced at a rate determined by the gamemaster.

### Reality Impaired
**Bonus: 5 BP**

The character is so accustomed to the Matrix and AR that he has lost any sense of what is real and what is virtual. The character tends to mistake real objects for AROs, and vice-versa, resulting in quirky mannerisms such as touching people in an attempt to call up information windows, ducking to avoid AR banners, or trying to delete physical objects. This bizarre behavior results in a –1 to all Social Skill Tests when in the physical world (as opposed to VR or astral space).

### Virtual Personality
**Bonus: 5 BP/level**

The character is only comfortable when wrapped in the anonymity of the virtual world. When not interacting with others as an icon, the character suffers a –1 dice pool modifier to all Social Skill Tests for each level of this quality taken (max. 3). May not be taken with the Chatty quality (p.36).

### Wild Technomancer
**Bonus:** 10 BP

The character is technically a technomancer. Unlike most technomancers, this character is still confused or afraid of his abilities, and has not yet been able to find a stream (p. 136). Lacking a framework for his talent, he has some difficulty developing and controlling it.

This quality may only be taken by a character who has purchased the Technomancer quality. This quality may not be taken with any other quality that confers a Resonance or Magic attribute.

The character with this quality is a wild technomancer (p. 140). He starts with a Resonance attribute of 1 and may increase it like any other attribute, to a maximum of 6. He has a living persona, but does not choose a stream. He may not take the Paragon quality (p. 37). The wild technomancer also may not learn skills from the Tasking skill group, nor may he compile, decompile, or register sprites. He uses his Resonance x 2 to resist Fading.

The wild technomancer can lose control of his abilities in times of stress. Anytime he experiences great emotion—for example, when in fear for his life, having an orgasm, flying into a rage, or holding his baby child—the gamemaster may call for a Willpower (3) Test. If this test is successful, the character keeps his abilities and emotions in check. If not, his abilities flare in a burst of uncontrolled Resonance that has unpredictable and dangerous effects. These effects are determined by the gamemaster, but may include attacks on nearby nodes, destructive commands sent to subscribed devices, the creation of a wild sprite (p. 160), the temporary manifestation and use of an echo, or any other effect appropriate for a technomancer. These effects are never beneficial to the wild technomancer, but are almost always harmful or even life-threatening to him and any bystanders. Each outburst causes Fading equal to the wild technomancer's Resonance.

Gamemaster's should be careful that this quality is not abused as a way of becoming a technomancer "for free" and getting extra BP to boot. It should only be allowed for players who are serious about playing a technomancer and who are ready for the roleplaying challenge of a technomancer that is not in control of—and endangered by—his own abilities.

## NEW LIFESTYLE OPTIONS

Presented below is a new lifestyle option. For more information on lifestyles, see p. 261, *SR4A*.

### FULL IMMERSION

This lifestyle is for those who wish to live in a virtual environment all their waking lives. These people have literally left the meat behind and exist only as their digital personae. They trust the care of their bodies to medical professionals, who keep them on elective life support. Hydration, oxygenation, nutrition, excretion, muscle toning, and every other aspect of long-term care are handled by drones or trained personnel, all while the client interacts with the rest of the world via VR or by jumping into drones. A character with this lifestyle also enjoys the benefits of the Hospitalized lifestyle, but must still cover extra costs for treatment or surgery.

**Cost:** 30,000¥ a month

## TWEAKING THE RULES

Gamemasters and players may agree to alter some of the rules of *Shadowrun* to better fit their playing style. These suggestions may be appealing to your group.

**Using Attributes**

Rather than relying on technology to determine a character's efficacy in the Matrix, Attributes may be factored back into the various tests in the Matrix. To do this, replace the program or complex form in each Success, Opposed, or Extended Test with the appropriate attribute (usually Logic). The maximum number of hits (not net hits) that can be generated by each Matrix Test is limited to the rating of the program or complex form in a manner similar to the way Spellcasting hits are limited by the Force of a spell (see *Force,* p. 182, *SR4A*). Agents, IC, and sprites would use their Pilot rating in place of the attribute required.

Alternatively, the various Matrix Tests can remain unchanged. Instead, the attribute (again, usually Logic) limits the hits (not net hits) of every test in the same manner described above. In either case, each Matrix Action requires the use of the appropriate program.

**Limiting AR Passes**

To make VR Matrix use even more advantageous over AR, the number of Initiative Passes allowed to AR users may be limited as far as Matrix use is concerned. To use this option, only one Matrix Action per Combat Turn may be performed when using AR, regardless of the actual number of Initiative Passes the character may have.

**Harder Encryption**

In the world of *Shadowrun,* cryptanalysis (the study of cracking encryption) is far more advanced than cryptography. To bring the encryption of the 2070s into line with current, modern cryptography, simply increase the interval for all Decrypt Extended Tests from one Combat Turn to one minute, or one hour, or even one day or one week.

Unless it is intended to make secure subscription links very safe, this should not be applied to signal encryption (p. 65).

**Tactical Cybercombat**

For games that would benefit from more tactical options in cybercombat, change the interval of the Extended Test for the Crash Program action to one Complex Action. Note that this does not apply to the Crash OS action.

**Security Tally**

Some groups may want to simulate Matrix systems that slowly become aware of an unauthorized user, rather than using the "breaking into a warehouse" analogy. The node accumulates hits toward an Extended Test threshold; the number of hits accumulated in this test is called the *security tally.* When an intruder first successfully hacks into a node, add the number of hits the node had accumulated in its Analyze + Firewall roll(s) to the security tally. Then, every time the hacker performs actions for which she uses the Hacking skill, the node makes an Analyze + Firewall Success Test and adds the number of hits to the security tally. If at any point the security tally reaches the threshold of (14 – node's System), an active alert is initiated against the hacker.

A hacker may reduce the security tally by Editing the access log, as she would normally. Under the security tally rules, however, rather than making a specific Edit Test, every hit on the test reduces the security tally by one. If the security tally is greater than zero when the hacker logs out, there is enough information to Track the hacker (as in *The Access Log,* p. 65).

**Complex Forms**

While technomancers are not magicians, some players and gamemasters may wish to bring the rules for the two closer together. To accomplish this, treat each complex form as though it were a spell, with no ratings and with the same cost in BP and Karma as spells for magicians. Then, when performing Matrix actions with the complex forms, the technomancer chooses a rating for the complex form, up to twice his Resonance. The technomancer uses the complex form normally, and resists a Fading DV equal to half the rating chosen (rounded down); this Fading is stun unless the rating chosen was greater than the technomancer's Resonance, in which case it is physical.

**Fading from Tasking Skills**

Compiling, Decompiling, and Registering can have capricious consequences when it comes to Fading. Sprite ratings normally considered safe for a technomancer can occasionally cripple him. To "smooth out the curve" of Fading due to the use of Tasking skills, change the Fading DV to half the sprite's rating (rounded up) plus the number of hits generated by the sprite in the Opposed Test.

**Alternate AR Bonus**

Instead of a straight bonus determined by the gamemaster, the bonus granted by augmented reality is dependent on a character's commlink. Rather than taking a set bonus, make a System + Response Test. Every hit garnered grants a +1 bonus from the character's AR, as a Teamwork Test (see p. 65, *SR4A*). A glitch may indicate anything from slightly faulty information to a spam ad opening over an important part of the heads-up display.

**Loss of Resonance**

Like otaku before them, technomancers' abilities may be tenuous. For a game that is harder on technomancers, gamemasters may include the risk of Resonance loss due to any or all of a number of conditions: rolling a glitch while resisting Physical damage or Fading, being the victim of a glitch by someone performing medical treatment on the technomancer, severe electrical trauma, excessive disconnection from the Matrix, or even aging further and further beyond puberty. This loss affects both the current and maximum Resonance rating.

# . . . THE IDIOT'S GUIDE TO THE MATRIX . . .

SueZ pulled at the edges of her dress as she squinted across the virtual dance floor, a futile effort to modify her icon's appearance. She knew it had been a mistake to let her boyfriend play with her commlink, but she couldn't wipe her ID trail or radically modify her profile on her own. Her off-the-rack avatar wouldn't have been allowed access to this place, so she needed him to reprogram her usual boring goth-cheerleader look. As a result, her social debut saw her wearing something that looked like a Victorian trid show period piece made entirely from vinyl. Next time she saw him, they were going to have a talk about taste.

She tried to summon up an aura of confidence she didn't feel. If her parents caught her doing this she would be very, very dead. SueZ reconfigured her emotive filter to hide her nervousness and slipped between the various ... things blocking her path. The first advice she'd heard about this place, long before she found the hidden path to its doorstep, was to mind her manners. She was sure she could clip right through most of the "people" chatting to each other in the club, but she was just as sure she didn't want to anger the natives.

The natives were definitely the most interesting part of the club. The appearance of the space changed on a regular basis, but it wasn't anything cutting-edge. Tonight the club resembled a dimly lit dive bar out of ancient history. Brassy music blared from the speakers, and the simulated smoke and smell of tobacco floated through the air. The patrons, by contrast, ranged the gamut of avatar sophistication. One user had painstakingly created a pudgy middle manager, right down to the dandruff on the shoulder. He was speaking to an animated creature of fire and lava wielding a spiked battlehammer. Well-crafted, but not the avatars SueZ was seeking.

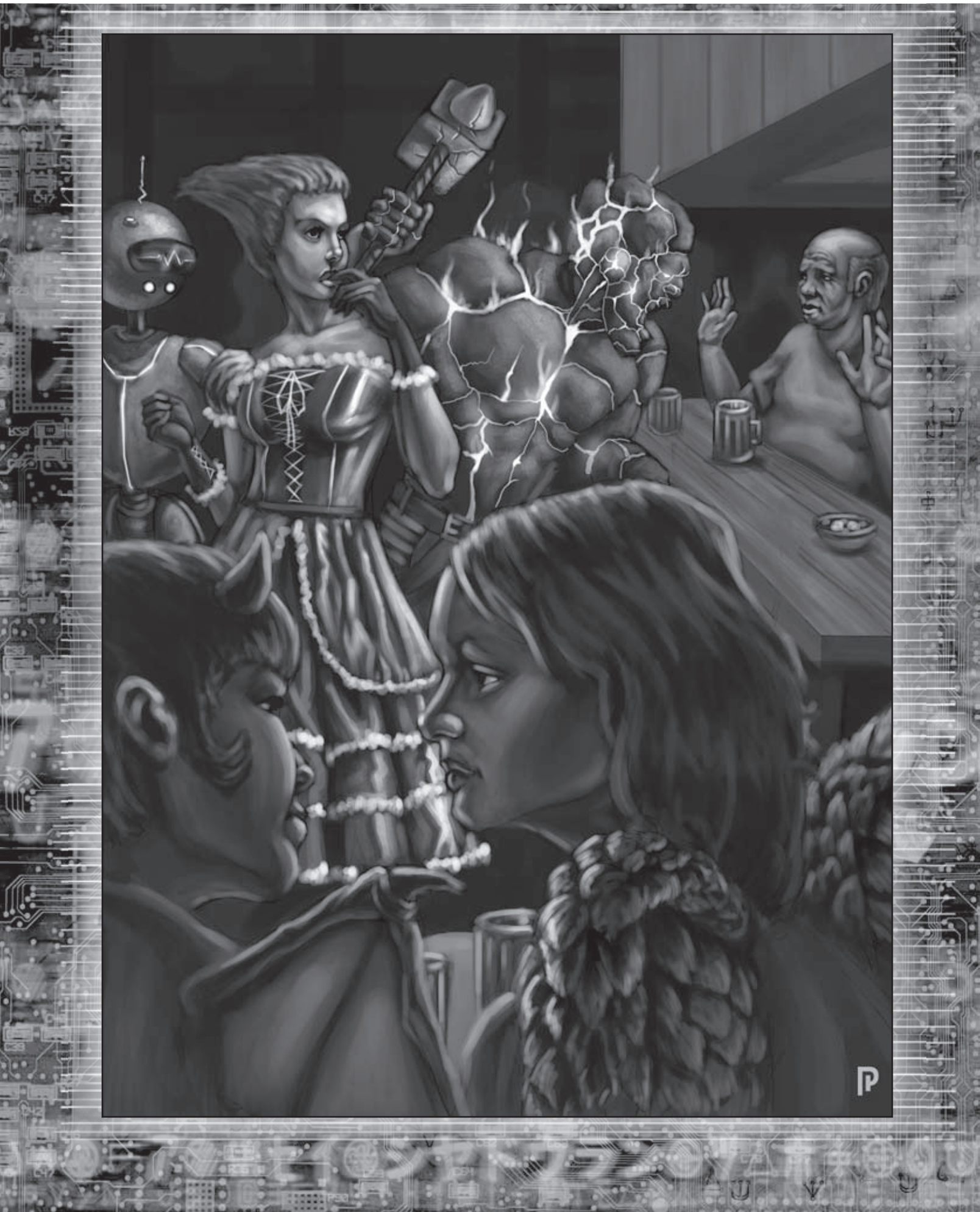
In the shadows by the bar, a pair of trim avatars waved in her direction. The one resembled some sort of winged she-devil, all leather and spikes, while the other had soft white feathered wings and a halo glow around her head. The two moved in mirror image to each other as they drew SueZ near, guiding her closer to the bar. The bat-winged avatar smiled, and handed her a simulated drink. In her hand the glass was cold, and in the glass swirled a purple concoction swarming with damned souls.

"Off-the-rack tech, ne?", the angel asked with the echoing voice of a choir.

"Y-yes. Sorry. I, um. I have it." SueZ held the glass tightly, staring at the swirling faces in the brew. "Can you get me out?" The women exchanged glances.

The demoness leaned close. She smelled of brimstone. "You will get us your parents' pass-keys?"

SueZ took a deep draught of the purple liquid, nodded, and said "Get me out of the arcology, and I'll get you whatever you need."



# USE THE MATRIX BEFORE IT USES YOU

**Posted By:** RazorOfLove

» Ever had an annoying shaman that couldn't understand digital security protocol if his life depended on it, even though you explained it a thousand times? If only you could tell him to read the fuckin' manual. Well, here's a fuckin' manual to pass to your teammates; it's what I pass to mine. This looks like it was written for tweens, and it was, but it was written by a hacker with some real chops. She was a Matrix Science teacher before dropping into the shadows, and yeah, she was my teacher once. She said that she wouldn't teach me how to hack, but if I paid attention I would learn, which is the way it works.
» Slamm-O!

» Is it just me, or is this file size too big for its contents?
» Hannibelle

» Nice catch. Razor used steganography to include Glitch's Hacker's Handbook as an easter egg for kids with the skills to pry it out.
» Slamm-O!

Congratulations! You're probably reading this because you're old enough to leave your KidLink™ behind and get your own fully-featured commlink. There's a big bad virtual world out there for you to explore, but if you're not careful, it will eat you up and spit you out. Not to worry, you're reading this guide, and soon you'll be surfing the digital waves with the best.

## THE BASICS

The first thing you're going to need is a commlink (duh). You're also going to need an operating system, or OS. Always try to get the best commlink model and OS you can afford. The electronics store is not a place to skimp in a wireless world.

You're also going to need some interface gear. Sure, you can use the commlink's built-in screen and thumb-buttons, but that's pretty lame. Get an image link so you can see AR objects and data; it can be built into shades, regular glasses, goggles, or even contact lenses for that natural look. Grab some ear buds or headphones (depending on your look) so you can catch your tunes and other audio. A microphone will let you make commcalls without having to use your 'link's mic. Add some AR gloves to complete the ensemble; you can get them as gloves, paste-ons, or even as a set of full-finger rings. Whatever your look, you can use the Matrix in style.

### Direct Neural Interface

Be wary of people who tell you that DNI is the only way to fly. You might think that you can get a datajack even though it's illegal in most places to buy a DNI before you're 18 or 21, but be careful. You're probably not done growing, so a datajack is not a good idea yet. But even with trodes, DNI is a gateway directly to your brain, and a person can get seriously messed up through that interface. Nevertheless, the ability to simply think your commands is an incredible ease-of-use factor that makes trodes worth the risk.

To roll with a DNI trode interface, you'll first need to spend a few minutes configuring your trodes to your brain the first time you use them. Your trodes will slave themselves to your sim module, and then your commlink will give you a series of mental exercises to do. Don't come crying to me if something nasty happens to your wetware.

### Getting the Hook Up

Chances are, your family, enclave, or arcology already has a Matrix service provider, or MSP. Despite what the ads say, you don't really need an MSP to get onto the Matrix, your commlink has all the hook-up you need. But MSPs provide you with storage space and a messaging service that will hold on to your messages when you're offline, not to mention programs (usually Browse class programs and Edit class programs) that you would otherwise have to buy yourself. The more expensive ones let you use agents to do things for you.

### Call Me, Baby

One thing an MSP is good for is to get a commcode. You need a commcode if you want people to be able to call you and send you text, image, and voice messages. Some MSPs will give you more than one. If you don't use an MSP, you can get a commcode from any number of providers.

Don't give your commcode to just anybody! Once it's in the hands of a marketing node, your commcode will be on a hundred thousand spam lists.

And don't worry about getting software to make calls. All the stuff you need to chat with your buddies is built into your OS. Speaking of programs ...

### A Hard Look at Software

You might want some programs if you don't want to rely on an MSP. You can buy your own Browse class and Edit class programs and load them into your commlink. If you play a field sport like lacrosse, hockey, or football (either kind), your coach will give you a TacNet class program unless you're in a classic-rules league. I also recommend an Encrypt class program, you can talk to your friends without your parents eavesdropping.

One program that is a must-have for your commlink is an Analyze class program. Keep it running as often as you can. It helps against hackers and lets you check out icons to see if they're harmful. I recommend WhatsThat from the Matrix Open-Source Syndicate; it works and it's free!

» This is a little out of date. MOSS was bought up by a subsidiary of Evo, so now WhatsThat costs around 200¥. But the advice is still good: always keep an Analyze program running.
» FastJack

There are other programs out there that let you do other things, but those are up to you to find and figure out. But remember: if you don't have a program for what you want to do, you can't do it, so load up that commlink!

### Work Those Programs

Loading a program into your 'link doesn't mean you can use it. In order to use a program, you've got to run it first. Running programs takes up processor time and memory space in your commlink, and if you run too many programs, your 'link will s-l-o-w

d-o-w-n, big time. The better your OS, the more programs it can handle at once (I told you not to skimp!).

You might want to run an agent or two (who wouldn't?). Remember that those agents are programs, too, and cause the same slow-down that other programs do. Not to mention that the programs the agents use have to be running along side them. Another thing to remember is the one-user limit: you and an agent can't share the same running program. If you've got a program loaded, you can run two copies of it as long as the agent is yours, too, but that's even more programs to slow your commlink, so don't go crazy on the progs.

Now that you're loaded up, let's take this puppy for a test drive ...

## SURFIN' THE 'TRIX

The Matrix is a virtual place. Technically, it's a synthetic hallucination that is expressed using the analogy of geography by consent of its users. Which is the scientific way of saying that it's only a place because we've decided it would be. All those nifty virtual landscapes you've been looking at? All fake, phony, and not there, not even a little bit. Somebody's imagination on steroids.

What does this mean for you? Absolutely nothing. The Matrix was designed to appear to be a physical location on purpose, so if you treat it like it's a place, everything will work just fine. But the Matrix isn't just an imaginary place, it's a bunch of imaginary places.

### Nodes and Icons

The Matrix is really made up of a whole bunch of nodes. A node is a virtual location that represents a Matrix system. Everything in the Matrix is either a node or in a node. In fact, your PAN (that thing we set up with your commlink and peripherals) is a node, too!

Everything else in the Matrix is called an icon. Every file, user, agent, datastream, device interface, everything has an icon. Icons usually look like things, and you can touch them to interact with them, just like in real life. Everything in the Matrix that isn't a node is an icon (yes, even technomancers).

• That's not entirely true.
• Icarus

Things in the Matrix are designed to look, smell, feel, taste, sound, and act a certain way. This is called sculpting. A node can be sculpted to look like a church, a classroom, a beach, or even empty space. Icons are sculpted, too.

Don't worry about not being able to tell different icons apart from each other and from the node. Your commlink will identify which objects are icons and which are just pretty background.

• This is where Stealth programs do their work. It's impossible to make your icon undetectable in a node without getting disconnected, but it is possible to make your icon look like something innocent.
• Slamm-0!

### Less Talking, More Surfing

Okay, let's have a look. You're currently just look at things in AR mode, which means you have a couple of small windows open to the side of your field of vision. Note how in AR, everything is depicted as small icons, small amounts of text, and small trid clips? And it's all transparent, so you can see what's happening in the real-world too? That's because that's the point of AR, to let you interact with the meat world and the Matrix at the same time.

First off, mental click on that icon to the right, and take a closer look at the expanded view. That's your current icon. When people see you in the Matrix this is what they'll see. Unless you got a really cheap OS, you'll have hundreds of different options to play with. Go ahead and sort out your first look, I'll be here when you're done.

All set? Okay, now see that window on top, the one with the logo on it? That's your commlink icon. Mental click on that and drag it to the center of your vision. Now mentally toggle over into virtual mode. See how it shifted from an icon to a window? Through that window, you're looking at the default sculpting of your OS, a bare-looking room with a logo on it. This is what your commlink node looks like in VR, only we're still viewing in AR so you see it like you would presented on a display screen. VR is a whole different experience—if you were in VR, you'd actually be there, completely immersed in that environment. It's not a real place, but it might as well be. Don't worry about the decor right now, you can futz with it later.

Now, let's check out the 'Trix. Start by mentally clicking the icon that says "local grid." See the window that popped up with a big list of names? Those are all of the local nodes within wireless range. Now look back to the virtual view window, and you'll see the point of view has changed so that you're now floating above your node, which probably looks like a box with the same logo (you can fix that, too). This is a spatial representation of the nodes that your PAN can access directly. Straight down is your node, and there's probably your household node nearby (unless you're not at home, natch). Maybe some neighbors' nodes around, and possibly some others. You might see some moving nodes that belong to passersby or vehicles outside. You can probably see a lot of advertising, too, floating here and there. Nice view, huh?

Ok, pop up a search window and look up the address for your MSP, or just select it from that node list. Hit the connect button. Bam! You've just accessed the public area of the MSP's nexus. If you were in VR, you could have just flown over (or zoomed in on) and touched the MSP node's icon. By convention, they're usually sculpted as towers (but then so are nodes for actual towers, so if you live near a tower, it could get confusing). In the virtual view window, you can see what the inside of this node looks like in VR. Pretty wild and noisy, huh? Go ahead and look around, you can't damage anything here, and you certainly won't crash the 'Trix.

• You can't crash the Matrix. In fact, the unwired version of the Matrix is made up of independent nodes sharing information. If another crash is imminent, all of the "safe" parts of the Matrix will isolate themselves and localize the crash. The Matrix is uncrashable.
• Clockwork

• "Uncrashable" sounds a lot like "unsinkable."
• The Smiling Bandit

About this time, you're probably getting your first spam, unless you've got a really good firewall. Spam's not dangerous,

and most of the time your OS pushes them to the edge of your view, but they can get annoying. You'll only encounter extreme spam in heavily-trafficked areas (both in real life and the Matrix). Trust me, you don't want to buy anything from a spammer, so just let them open, do their thing, and close again.

You don't actually need to see all this wild bedlam, so this would be a good time to start playing with your filters. Look for a funnel or sieve icon, or the "filter" kanji (if you're using DNI like I told you not to, you'll need to think it; it might take you a few tries). Select (or think) "Remove Traffic" from the menu that pops up. That should calm things down a bit in the virtual view window. Now your commlink has stopped rendering network traffic. It's still there, but you don't sense it any more. You can be as selective as you like with your filter, and even "fly blind" by filtering out everything but the scenery. Try out some different settings; you can fine-tune it later.

If you're done playing around with the MSP's node and your filters, look around for the regional link. It usually is sculpted in the form of a globe or a map. Use your Analyze program if you're having trouble sorting out which icons do what. Now touch the map and activate the regional view. Yow! An even bigger list of nodes has popped up! This is all of the nodes that the MSP is aware of, and that's usually in a big area. You can go to any of these nodes you like, although you'll only be able to get into the public areas (and most of those just say "go away" or a variation thereof). Later on, you can bookmark or fave nodes that you like, so you can just go straight there instead of hunting for it.


If you want to get into a node properly, and not just its public areas, you'll need an account on that node. Then you'll be able to get inside the node and use whatever the owners allow you to use.

» For those who are less than Matrix-savvy, when we're hacking a node, we're creating an account for our own use. The more access this hacked account has, the harder it is to create.
» The Smiling Bandit

Let's try a public library. Open a search box and find one. Then go to it and sign up for an account. It will access your SIN information and get you hooked up.

Check out how the virtual view of the node changes when you get your account. You're on the inside, baby! You can check out books and videos and stuff later, but first notice how big the place is. It's actually bigger, but there's stuff here you can't see. Just like stores and things have back rooms, nodes have private areas that you can't even see without a higher-level account. In fact, there are probably icons for things you can't access floating around right now. Don't worry, if your 'link can't detect it, it can't interact with you, either.

Okay, that's your training flight. Go play around or buzz your friends' home nodes or something. Don't be afraid to try things, a node won't let you do anything it doesn't want you to do. When you're ready to find out more about the Matrix, keep reading.

## FACE TIME

Now that you're loaded up and running some progs on your 'link, let's get out into the wide world of wireless. The Matrix is a big place, so you'll not only be able to keep in touch with your current friends, but make new ones around the world. It's not all fun and games, though; there are some freaks and dangers out there, but if you follow my lead and surf smart, you'll be able to use the Matrix before it uses you.

### You've Got the Look

You get to decide how people see you in both AR and VR. The technical term for what people see when they look at you in the Matrix is "icon," but a lot of people call it your avatar. There are literally thousands of icons available from stores, "off-the-rack" as it's called in the Matrix. You can get pretty much any one you want, and all of them come with customizable detailing.

If you really want to stand out, though, you use a custom icon. Custom icons are hella expensive, but totally wicked, and guaranteed to be unique. If you've got an artistic bent, you can make your own icon, too, but you'll need a good Edit-class pro-

gram and a massive amount of time (every single action of your icon has to be programmed, animated, and pre-rendered).

### Commcalling

You've been able to get commcalls on your KidLink™ already, but now you'll be able to call anybody, not just the people your parents okay. When you make the call, you can specify audio, text, image, video, or any combination of the above. Just pick the commcode of the person you're calling, hit the commcall button (or whatever you've set up for your personal commlink), and wait to connect. If you don't need to talk to them right away, just compose a message, in voice, text, or images or whatever, and bam, you've sent an email.

Now that you have a real 'link, you'll also be able to call more than one person at once. You don't even have to have all of the conversations at once. You can hold some, merge others, only send messages to part of a group, whatever you want. The power is totally in your hands!

Remember that while you can call anybody, anybody can call you, so always screen your calls before you connect, and leave the auto-answer feature alone!

### You Are Who You Know

One of the coolest things you can do on the Matrix is connect with your friends on social sites. There are a bunch to choose from, like blog hosts, interest clubs, forums, info boards, and so on. They offer chat proxies (so you can call people without giving out your commcode), file sharing, and discussion groups where you can post your thoughts and read those of others.

A social network can help you out and help you find folks who can do you favors, but don't forget that it's all give-and-take. Every social network has a reputation system of some sort, be it ranks or smileys just a number. If your reputation is low on a site, you're not likely to be popular, and if you ask for too much you might get kicked off, so be polite and lend a hand when you can.

### Awesome Places to Be

There are some sweet clubs, hip-hoppin' hang-outs, and neo-rawkin' raves going on in the 'Trix. These places are just like real-life clubs, except that all the architecture is virtual. Jump in, pop your AR to full-view (you still aren't using VR, right?), and enjoy.

These are the places where your icon can be important. They are the best venues to see and be seen, whether you're wearing off-the-rack or a custom number. In fact, if your avatar is good enough, people won't immediately assume you're a kid and not take you seriously (yeah, grown-ups suck, I know). Some places won't even let you in if your icon isn't up to snuff. A lot of places will disconnect visitors who misbehave, too, so mind your manners!

It's true that you could go to these places in VR. I'd hold off on the whole virtual reality thing, but if you're going to do it, read what I have to say about it later on before you jack in!

### Keep Your Friends Close and Your Enemies Pwned!

You da playa? Got game? Prove it over one of hundreds of massively multi-player games! You can find pretty much any kind of game you're looking for, from Miracle Shooter to Pony Trainer and everything in between and on either side. Be careful not to get into it too much, though, 'cuz the stories about kids dying because of an AR game aren't all urban legends.

- She's right. They're not.
- Snopes

### The Matrix Knows Everything

Almost the whole of human knowledge is sitting on the 'Trix, waiting to be found. You'll need a Browse program of some sort, but your MSP has one, if you have an MSP. Most databases aren't free, but a lot of them will come with your MSP. For the others, you might need an account. Aetherpedia is a good and comprehensive database of information about everything under (and around) the sun, and it's free if you have any kind of MSP.

- Aetherpedia's got an augmented wiki-style editing and peer review scheme, so it's always a good place to start. Plus it's trivial to hack if you don't have an MSP.
- Glitch

### But Wait! There's More!

There are all kinds of services and surprises available in the Matrix. Data havens, hidden clubs, meta-games, blogs, escrow services, newsfeeds, you name it, it's probably out there.

- Data havens? Isn't this for kids? And escrow services? Why the heck is she talking about escrow services?
- Kane

- She's probably planting seeds in the minds of future shadowrunners. The employers who are up-front about paying will set up an escrow account with a trusted entity, usually your fixer. That way you know you'll get paid, and the issue of trust is never raised.
- Fatima

- Another way to gauge Mr. Johnson's credibility is to ask that they use an escrow service to insure payment after the job is complete. If they balk, you walk.
- Haze

But that's not all that's out in the big bad virtual world ...

## THE DANGERS

There's more to the Matrix than data searches and a social scene full of awesome. There is a lot of bad stuff out there, and if you don't play it smart, it'll chew you up and spit you out. The 'Trix ain't for kids. Don't worry, though, just read my warnings and stay smart, even if your friends aren't. Don't be a statistic!

### Brainfried

You can read it in the newsfeed almost every day. Some kid gets brainfried on DNI. That kid thought that it could never happen to them, but there they are, brain dead and drooling. DNI can mess you up hard, before you can blink. You don't need it. Everything you can do in VR you can do in AR.

But if you're not going to take my advice, then at least don't be an idiot about it. Use trodes instead of an implant, so you can take them off if things get dangerous. If your 'link suddenly starts the configuration process with your DNI again, take them off and reboot, you've been hacked. And never go solo; make sure there's someone there with you to pull the trodes if things look bad.

In today's Matrix, you don't have to use VR at all. You really shouldn't. But if you're going to do it anyway, always do it in a safe place with people you trust. You might think that you can handle it, and you're probably right, but you can be dead right.

» I've seen a copy of this in a public school, except it had all of the information and warnings about DNI stripped out, as if not telling kids about it would keep them from doing it.
» Butch

### You Got the Power

There are plenty of hackers out there that might want to get into your commlink. They have different reasons: curiosity, data mining, marketing research, or they're just mean or homicidal. They have tricksy ways of getting into your 'link, too. It might look hopeless, but you've got an ace up your sleeve.

Find your commlink's power button or switch and make sure you can find it by touch. Hackers can't hack what isn't on. The moment your 'link starts to act funny, or an icon shows up in your node without your permission, hit that power switch and report it to the authorities (your parents, a teacher, the police, whoever). Hopefully, by the time you reboot, the hacker will have gone to look for easier pickin's.

» They trained us on this in Knight Errant. If we thought we'd been hacked in a firefight, we called a "10-30," found cover, and rebooted.
» Sticks

» If your OS has been hacked with a backdoor, this will only delay the hacker while you reboot. If it happens to you, and you can't code, you can only fix it by reinstalling your OS.
» The Smiling Bandit

### Analyze This

Use that Analyze program on everything. If it's a strange icon, do it twice. Most of the icons in the Matrix are safe, but some are nasty and out to get you. The bad ones might have a "Stealth" program that will make them look like normal, safe icons, so be especially careful when you don't know the person behind the icon.

### Iconism

The good news is that when the world only sees your icon, they can't be prejudiced about your metatype, gender, race, age, or anything else. But folks will judge you on your icon. It's like extreme class discrimination, except that it's based on your software. What passes for acceptable or contemptible changes depending on which node you're in, so don't let yourself get ambushed by digital bigots.

» The reverse is true, too. If you want to blend in, switch to an off-the-rack icon.
» Puck

### Spam Spam Spam Spam

Most of the time, spam is just annoying. But some of it can carry viruses and other buckets of digital nasty. Never run a program attached to spam, ever. Keep that firewall up, and whenever you can, drop to passive mode.

### Blog Smart!

Keep your personal information out of the public eye. Don't give it to anyone that isn't a cop, teacher, or other person who will keep it safe. Once you put something onto the Matrix, it's on the Matrix forever.

## GET READY TO RAWK

By now, you should be soaring through the Matrix like a natural. If you're not, don't worry; it'll come. Now go out there and shake up that 'Trix. You'll have freedom that you've never had before. Enjoy it, but be careful. With great power comes great responsibility.

Be good, and if you can't be good, be safe!

» And if you can't be safe, name it after me!
» Glitch


Hex was flying some five hundred kilometers above the Earth. In the distance he could see the space station Treffpunkt Raumhafen, floating above the atmosphere. He was not alone. Two hundred kilometers away a dog was talking to a crystal robot. Hex zoomed in, and he could see the reflections of the dog's fur in the sparkling crystals of the machine. Hex was waiting.

Suddenly his left index finger was throbbing. He looked at one of the semi-opaque monitors floating in front of him—the ones only he could see. The video feed showed a man in a black suit with mirrored glasses walking out of a building. It was time to go.

The hacker, a bright blur of speed, approached North America, shifting to the regional telecommunication grid of the UCAS without a nanosecond's pause. Further on he sped until he stood in the Seattle Matrix in front of a shining cab gleaming with emerald fire. This cab would take him to his destination, a private network. He entered the taxi and darted through a data highway until he reached a distant field with a setting sun. A farmer approached, asking for goods to trade. Hex produced a hay cart from his pockets and offered it. The farmer nodded and went to work on the crops in the field.

Hex strode on towards the farm. It consisted of a barn, a main building, and a small cottage. He mentally ran through a short series of instructions, and small descriptions appeared next to the buildings. A man in blue working clothes came out of the barn. Hex reached into his pockets and drew out a small magnifying glass. He watched the worker through the glass and read the long lines of data materializing in the air. The man in blue was just another persona.

With another mental command, the scenery instantly transformed. The buildings turned into small gray blocks with fine black lines in between, pulsing with the light of data traffic. The fields around him shrank to a large room with only one door where the road had been. Hex's reality filter had stripped away the useless and the nonsensical, translating the look of the network to the bare information-content he preferred.

The hacker analyzed the room he was in, the node acting as network hub. Seconds later he had cracked his way into the hub, reading the node descriptions reserved for security users and adding further information to the labels of the network's nodes. The former barn, now just a gray block, turned red, showing it to be a security node. A small plate fingerprint scanner marked the entrance.

Hex smiled. Sometimes it was just too easy. He pulled out a gun and fired at the scanner. The block started to glow in red light. Active alert. With a grin that never reached his physical body Hex logged off the node.

# HARDWARE

The basic building blocks of the Matrix in *Shadowrun* are devices of varying processing power (see *Nodes,* p. 57) and their interactions through fiberoptic cables, radio waves, satellites, and sometimes laser or microwave links (see *Data Exchange,* p. 53).

In 2070, almost everything carries some kind of node with it. Whether it's RFIDs in clothes, small processors in refrigerators, commlinks in jewelry, or full-blown servers in huge racks, nodes are all over the place. The air is constantly filled with a buzz of radio waves, coherent signals directed at satellites, and fiberoptic cables pulsing with the light of data transfer between continents. In short, the Matrix relies on the hardware that forms its parts—a fact that was known before the Crash 2.0 but often overlooked.

## NODES

Nodes are the most important building blocks of the Matrix. Every computerized device able to execute programs and instructions is a node. They provide the raw processing power of the global network and are the places of the Matrix (see *Sculpting*, p. 55). Everything governed by standard Matrix protocols happens in nodes. They run programs, store data, accept connections, and run personas and agents. Each node is governed by an operating system, from which it derives its Firewall and System attributes (see *Operating Systems,* p. 51). Its physical hardware components determine its Response and Signal attributes.

There are three general categories of nodes: peripheral nodes, standard nodes, and nexi. Apart from the four Matrix attributes, a node is characterized by its access ID, persona limit, and processor limit.

**Access ID:** Every node has a hardwired access ID, which serves as its address in the Matrix. If someone wants to find a node, they look up its access ID.

**Persona Limit:** This is the maximum number of persona that may simultaneously run/originate on the device. Note that this only counts users who are using this node to get online, it does not count persona running on another node that access this node.

**Processor Limit:** This is the number of programs the node can run before it starts to experience Response degradation (see *Matrix Attributes,* p. 221, *SR4A*). For standard nodes, the processor limit is equal to System rating.

### Peripheral Nodes

Peripheral nodes, or peripherals, and the devices they run on can be found in almost every single item in 2070. Peripheral nodes are common in objects that don't require the computing, processing, and networking capabilities of standard nodes, but that benefit from being networked or accessed in some way. RFIDs carry peripheral nodes; toasters, fridges, and guns contain them; and even clothes facilitate peripheral nodes to process information.

Peripherals use the same rules as standard nodes (see *Nodes,* p. 224, *SR4A*), with some restrictions. They are only able to run a single persona and can only run programs they are designed to use. Matrix attributes of peripheral nodes range from 1 to 6 just like standard nodes, though most peripherals have low Response ratings. For simplicity, most peripheral nodes are given a single Device rating to represent all of their Matrix attributes (see *Device Rating,* p. 222, *SR4A*), but gamemasters should feel free to adjust ratings as they feel appropriate.

Since the operating systems of peripheral nodes are far more limited and focused, their System rating is not restricted by the Response rating, as is the case with standard nodes. In other words, the System rating of peripheral nodes may exceed Response rating without penalty.

Peripheral nodes can only run one persona at a time, they are not designed for multiple users. For this reason, they only have admin accounts, but these accounts do not receive the +6 threshold modifier for hacking (treat them as standard accounts). They can, however, be clustered with other minor nodes, acting in concert as a single super-node (see *Clusters,* p. 55). To guard against their weak security, peripheral nodes are often slaved to more secure nodes (see *Slaving,* p. 59). Other functions, like data storage, communication with other nodes, or the representation of peripheral nodes in VR, work exactly like standard nodes.

#### SAMPLE PERIPHERAL NODES

| Device | Response | Signal | System | Firewall |
|---|---|---|---|---|
| AR Glove | 2 | 2 | 1 | 1 |
| Credstick | 2 | 2 | 6 | 6 |
| Fridge | 1 | 3 | 2 | 1 |
| RFID tag | 1 | 1 | 1 | 1 |
| Security Camera | 2 | 3 | 2 | 4 |
| Smartgun | 2 | 1 | 3 | 4 |

### Standard Nodes

Standard nodes are run by commlinks, terminals, home telecoms, and almost any object that is portable and capable of running a single persona and a number of programs or agents.

Standard nodes use the rules given for nodes (see *Nodes,* p. 224, *SR4A).* They have standard processor limits.

Standard nodes may only run a single persona at a time, but the interface allows individual users to tailor the persona to their particular settings and preferences.


WARNING!
CHECK ENGINE
TOMORROW'S WEATHER
77/45 QUAKE WARNING
TURN RIGHT AHEAD
ACCIDENT REPORTS
• avoid the corner of 6th & main
• gas leak on Woodward at 4th
• 5 car accident with fatality on North Ave west of Clybourn
D
P
40 MPH

### Nexi

Nexi is the catch-all term for high-performance mainframes, multi-user wireless workspaces, and high-traffic hubs able to run a larger number of programs than standard nodes. They are commonly used by Matrix cafés, civic wireless access points, corporate servers, businesses that need VR workspaces and security nodes (see *Slaving,* p. 59), data havens, and for other processor-heavy tasks. The servers that run nexi come in a wide range of sizes and processor power, from units the size of a modern-day laptop to a full-blown server tower. The more processor power needed, the more powerful and thus bigger the hardware of the nexus will be.

In game terms, nexi work exactly like standard nodes with a few exceptions. They have a higher processor limit, allowing for more active programs (with the exception of agents, IC, AIs, sprites, and e-ghosts, which are limited by Response per standard rules—see *Response,* p. 222, *SR4A*). Their configuration and design also means that System rating is not capped by Response. Nexi are designed to run multiple personas; their persona limit equals System x 3.

Nexi have a minimum processor limit of 10 and a maximum of 50.

## DATA TRANSPORT

In the world of 2070, data travels from node A to node B in various ways. The most common means of travel are radio waves and fiberoptic cables. While radio signals, better known as wireless traffic, are mostly used to supply the end user with data, the bulk of the long-distance data transfer is delivered via fiberoptic cables. Other, more exotic ways of transmitting data are also available. They include satellite linking and laser and microwave beams.

### Fiberoptic Lines

Contrary to public opinion, most of the data in 2070 is still delivered via fiberoptic cables. An optical fiber is a cable made of glass or plastic that is designed to guide light along a certain track. A carrier wave, mostly near-infrared light, is modulated to carry the information and sent through the cable to its destination at the speed of light. Compared to sending electric signals over a copper cable, fiberoptic transmissions have the advantage of being less prone to interfering effects and having much lower signal degradation even at high data rates. Fiberoptic cables run between continents, countries, cities, and even houses. Home telecoms, private access points, and most important, the access points of the large MSPs, provide the connection between the wireless and wired world.

### Radio Waves

When Joe Normal talks about transferring data, he talks about radio waves or wireless data transfer. Almost every single device in *Shadowrun* is able to broadcast data using electromagnetic waves of the radio spectrum. They require a relatively low amount of energy to produce, can penetrate buildings, cars, clothing, and other obstacles, and are easy to pick up. The biggest advantage and the reason for the tremendous success is ease of use. There is no need for cables in day-to-day life. No plug-and-play any more; in 2070 it's just play. All the cities throughout the world are littered with public access points that provide wireless access, linking people via the Matrix to almost any other spot in the world.

In places where access points are rare, either due to bad infrastructure or violent destruction, the user nodes themselves (commlinks, vehicles, etc.) provide access. The mesh network nature of the wireless Matrix allows every node in active mode to function as a router for other nodes around it. Data is routed from one wireless node to another until the next access point to the wired Matrix, or the wireless destination, is reached. In this way, even the Barrens are decently covered with wireless access points.

In both radio signals and fiberoptic cables, electromagnetic waves are used to transport data at extremely high speeds. A data request can easily make a trip to the other side of the world and back within 0.2 seconds.

### Satellite Links

Commlinks and other nodes can use a direct satellite link to connect to geostationary satellites and satellites in lower earth or-

### EXAMPLES OF STANDARD NODES

| Node | Response | Signal | System | Firewall |
|---|---|---|---|---|
| Standard Home Telecom | 3 | 3 | 3 | 3 |
| Premium Telecom | 4 | 3 | 4 | 4 |
| Business/Retail Terminal | 3 | 3 | 4 | 4 |
| Public Terminal | 2 | 1 | 2 | 2 |
| Civic/MSP | | | | |
| Wireless Access Point | 3 | 6 | 3 | 5 |

### EXAMPLES OF NEXUS NODES

| Nexus | Response | Signal | System | Firewall | Persona Limit | Processor Limit |
|---|---|---|---|---|---|---|
| Small Matrix Cafe | 2 | 3 | 3 | 2 | 9 | 10 |
| Large Matrix Cafe | 3 | 3 | 4 | 2 | 12 | 20 |
| Public Library | 5 | 4 | 4 | 3 | 12 | 50 |
| Online Shop | 3 | 4 | 3 | 4 | 9 | 15 |
| Matrix Backbone Hub | 5 | 0 | 5 | 3 | 15 | 50 |

bits (LOE). The advantage of using a *geostationary* satellite uplink is that your location cannot be pinpointed via trace any more precisely than a range of a few hundred of kilometers. This means that track programs are not able to determine the location of somebody using a direct satellite uplink. Unfortunately, the geostationary orbit is quite far away from earth (36,000 km), so data requests can be delayed by as much as a second. This second heavily affects and delays all Matrix interactions. The Response of a hacker using a geostationary satellite is thus halved (to a minimum of 1).

As an alternative, various *low-earth orbit* satellites are available. They require a tracker dish to follow the satellite and pick up another satellite when the original one comes close to the horizon. A typical LOE satellite is visible for about thirty minutes. They are fast moving, and the difference in signal travel time can be used to determine position much more accurately (using standard rules for track programs, p. 234, *SR4A)*. As they are much closer to Earth (less than 1,000 km), these connections are not affected by satellite lag.

#### Beam Links

Beam links are connections between a sender and a receiver using a laser or microwave beam to transport the traffic. A direct line of sight is needed to maintain the connection, and neither sender nor receiver may move. Beam links have the simple advantage of not being intercepted easily, but they require complex machinery. Laser links, however, are affected by environmental conditions like rain, fog, or clouds, which might lower the Response of a user by up to 3. Microwave links are not affected by environmental conditions.

## SOFTWARE AND DATA

Though nodes provide the stage of the Matrix, content is needed to bring it to life. Something has to happen on the stage and somebody has to do it. Software and data are the content of the Matrix, filling it with buzzing life.

### DATA

Almost everything Matrix users do revolves about manipulating, sending, processing, or creating data. Data is stored in various places, ranging from optical disks and chips to the hard drives of devices and servers. In 2070, everybody is able to record everything they do all of the time. This includes all their communications, e-mail, phone calls, trid-calls, blogs, websites, as well as an enormous load of sensory information coming from houses, cars, workplaces, clothes, and much more.

However, data in 2070 is not only data. It carries extensive meta-information of various kinds. The complete history of editors, generators, programs, dates, and versions of programs used, connections to other pieces of data like their location, search terms used to find the data, and much more is stored. Most of the time, the meta-information is larger than the data itself. This information is especially important for data mining purposes, searches, and bookkeeping. The amount of data available in 2070 is so vast that finding a particular piece of data and getting its context is often as important as the information content itself.

### OPERATING SYSTEMS

Operating systems are the programs that control the functioning of nodes. The OS manages resources and tasks, processes data and input, handles accounts and authentication, allocates memory, prioritizes requests, and serves as a platform for other software. It also provides a user interface in the form of the persona for each user.

Operating systems also provide controls for the physical device they are loaded on. Most OS's are customized according to the nature of the device, with various applications controlling different functions. An OS designed for a toaster, for example, knows nothing about doing laundry or making a washing machine work—but the OS for a washing machine can tell you details of its recent washing cycles, warn you about mixing whites and colors, alert you when you're out of bleach, and provide various setting controls.

Operating systems can follow their programming and any command inputs, but they are not capable of making complex decisions. If you want a node's OS to do anything that doesn't fall within its normal programmed routines, or you want it to follow a complex procedure, you need to write a simple set of commands called a *node script.* The OS will process the node script and execute the instructions as ordered. Node scripts are perfect for customizing a node's security response. For example, the OS can be instructed to launch IC, trigger an alarm, or send a message when certain conditions are met. Depending on the access rights needed to perform the action in question, any user can write and store scripts on a node. Hackers can abuse this to trigger certain actions at a later time or when a special condition is met. Writing node scripts requires a Software + Logic Test, with the threshold determined by the intricacy of the commands.

#### Constructs

*Construct* is a catch-all term for the entities in the Matrix that are able to make complex decisions, carry programs, and operate autonomously. The list includes, but is not limited to, personas, agents, IC, AI, e-ghosts, and sprites.

Due to their complexity, constructs need a constant stream of information to and from the nodes they are accessing (see *Subscriptions,* p. 55). Constructs can be attacked in cybercombat, and the programs carried by constructs can be crashed. (For more info, see *Autonomous Programs,* p. 110.)

#### Personas

Though personas are sometimes confused with operating systems, in fact they are the basic user interface an operating system provides by which you access the device and the Matrix—a so-called user shell. A persona is a combination control panel, web browser, email client, and more. It is an integral part of the OS, in that every operating system features a way for a physical user to access the device and get online. The persona's ratings are based on the OS, but they are separate things.

The operating systems of nexi (but not peripheral or standard nodes) can run more than one persona interface at a time, meaning that multiple users can use the same device to get online. Persona interfaces are designed to be used exclusively; consequently users may only control one persona at a time. While a user may have more than one persona running (on different nodes, devices or a nexi) it requires a Complex Action to change between different persona interfaces.

As a user interface for a particular OS, a persona is designed to be used exclusively—one persona at a time. While a user actually may have more than one persona running on different nodes or devices, each persona must be controlled separately. This means it requires a Complex Action to switch between persona interfaces

a user might have active on different devices. Users may attempt to control multiple personas at the same time at a +4 modifier to all actions for each persona after the first. As personas are user shells or interfaces for physical users, they are not designed to use node scripts.

Personas are intended to be interfaces for physical users and are not designed to use node scripts.

**Access ID:** Every persona is given a unique access ID. This is based on the hardwired access ID of the node, with an added signifier indicating the account. This access ID serves as the persona's Matrix address and is recorded by all nodes the persona interacts with, leaving a datatrail (p. 55).

**Subscription Limit:** The maximum number of subscriptions a persona may maintain at once is equal to System x 2 (see *Subscriptions,* p. 224, *SR4A,* and *Subscriptions,* p. 55).

### Pilots

Pilots are a special type of OS with more autonomous decision-making ability, used in agents and drones. Unlike operating systems or most other programs, Pilots are capable of operating independently and maneuvering through the Matrix on their own; see *Autonomous Programs,* p. 110. Like an OS, Pilots may also be programmed with sets of commands; see *Agent Scripts,* p. 100. Drone Pilots are also customized for the specific device they are made for (see *Pilot Capabilities,* p. 103, *Arsenal*).

## PROGRAMS

Programs are the tools of the Matrix. Every time something is done, a program is involved. Sometimes only a very small program is needed, and those instances are not covered by the rules—but it's still a program doing the work. Programs are always run by nodes. The maximum number of programs a node can handle is called its *processor limit,* while the number it is actually running is the *processor load.* If the processor load exceeds the processor limit, the node is subject to Response degradation (see *Matrix Attributes,* p. 221, *SR4A*). Programs do not have to be run by the persona's node to be used by a persona. It is possible to use programs run on the remote node a persona is accessing. The remotely used program then counts towards the processor load of the remote node instead of the node running the persona. Public nexi like libraries, archives, and data havens often provide remote browse programs.

# PROTOCOLS

Every time a node interacts with another node, predefined Matrix protocols are invoked. The receiving node looks at account data, access rights, and status of the connection and then decides whether a request will be accepted or not. By using hacking tools, hackers try to circumvent or exploit these protocols to again access rights, crash other icons, or do things not allowed by their current account privileges.

## ACCOUNTS

Access rights on nodes are governed by accounts. Every subscription and data request (see *Data Requests,* p. 54) is assigned certain privileges, depending on the account information that was sent with the request, or with the initial login in the case of subscriptions (see *Subscriptions,* p. 55). There are various flavors of accounts, depending on the status of the connection and what kind of information was sent.

### Standard Accounts

In the case of a standard account, the login data consists of a username and a password of arbitrary size. This information is always encrypted by the operating system, with a Rating of 6, upon sending. The password can be an alphanumeric string, a biometric pattern, or a signature produced by a passkey (see *Passkeys,* p. 64). The password is then compared to either the node's internal user database or other sources (see *Web of Trust,* p. 64) and either confirmed or rejected. Most users store their passwords or signatures in encrypted files on their commlink, as they are normally too long and complex to remember. Biometric signatures can be read directly from the user with the help of various types of scanners.

### Node Accounts

Node accounts grant access rights on nodes depending on the privileges a user has on another node it is linked to at that moment. User access on a security node, for example, might include a user account, and thus user rights, on the various cameras and sensors the security node is connected to. A spider working in the security node is then able to access all the sensors without having to provide the entire username and password data for the various sensor devices. The security node sends this information for him, and the spider can simply access the devices and control them. Or he could just read out their sensor feed as long as he is logged into the security node with the appropriate access rights.

### Access ID Accounts

Access rights can also be granted by access ID. This means that every time a node or construct with a certain access ID is accessing a node, it is automatically granted the access rights related to the ID. Just like standard accounts, the node compares the access ID with its internal user database and grants the appropriate rights upon initial login. A hacker can abuse this by spoofing his access ID (see *Spoof Command,* p. 232, *SR4A*) and thus forcing the node to automatically assign the related rights to the hacker.

## ACCOUNT PRIVILEGES

Access rights tell the node what the user of an account can or cannot do. In principle the administrator of a node sets the privileges related to certain accounts. Most nodes, however, tend to have the same categories of access rights. There are four levels of access rights: User, Security, Admin (see *Access Accounts,* p. 225, *SR4A*), and Public.

### Public Access Rights

If a connection is established without sending any information except the access ID, the connection is automatically granted public access rights. This is the type of access a user receives when she is entering the public part of a node. The public account allows access to public data like website information, blogs, databases, personal profiles, and so on. Depending on the accessed data, different access rights might come with the public account, for example the ability to write without a username in public forums.

### User Access Rights

The vast majority of accounts on a standard Matrix node are user accounts. The most important privilege normally granted via user access is one slot on the subscription list. This allows the user, or any of

his agents, to enter the node in VR or AR mode. Most other rights vary from node to node and from account to account. Depending on the purpose of the account, User accounts grant access to file indexes, files, the ability to edit files, command devices controlled by a node, upload data, common-use programs, and so on.

### Security Access Rights

Security access rights are mostly given to those who need more control over parts of a system without managing the entire system. This level is often granted to spiders, privileged users, and IC. They are allowed to view log files and node statistics and can alter general node attributes like a metaphor or special sculpting. Most of the time a user with security access is able to create or delete standard user accounts, edit other users' data, initiate (and deactivate) an active alert, and read the access log (see *Access Log*, p. 65). Security privileges also grant the ability to control and command all the agents or IC deployed by the node and run hacking programs.

### Admin Access Rights

The admin level is reserved for an owner or someone responsible for an entire node. Admin access grants the right to do everything the user wants to on a node. Admin privileges empower individuals to reboot the node, alter the node's sculpting, create and delete any possible account, assign access levels to accounts, and assign privileges to account levels. Furthermore, admins can view and edit all the log files and statistics available on the node, including the access log (see *Access Log,* p. 65). An admin cannot, however, affect programs and files he does not know about. He has to first defeat the Stealth program of an intruding agent that is running on the node before he can unload the unwelcome guest.

## COMMCODES

Matrix service providers (MSPs) issue commcodes (see p. 224, *SR4A*), which are not to be confused with access IDs. Whereas your access ID is a sort of serial number that you use for all of your interactions online, and which is recorded in access logs (like an IP address in real life), your commcode is more akin to a phone number or email address.

In principle it would suffice to call somebody by sending a phone request to the access ID of his commlink. The commlink would receive the request and the phone call could take place. On occasion, however, people buy new commlinks, leave their commlinks at home, in another room, or simply want to take their phone call, or any other kind of interaction, elsewhere.

That is why people register their devices at a Matrix service provider that issues commcodes. Matrix devices can be set to register with the Matrix service provider as soon as they go online. Every time somebody dials the commcode, the communication request is automatically routed through the database of the MSP that knows which devices are available to receive the call. Modern commlinks, house telecoms, and cars offer additional convenience by providing the MSP with the information on whether the user related to the commcode is present or not, so the incoming call can be relayed to the appropriate device.

## DATA EXCHANGE

In every data exchange, access IDs are used to guide the data from the sender to the receiver. The receiver then automatically

### BEHIND THE SCENES

So what happens when you get online? When you jack into or otherwise connect to your commlink (or any other device), what exactly happens under the hood?

Before anything, you must log on to the device. This presumes that you have an account on the device and a passcode (p. 225, *SR4A*) for accessing it. Some devices may have a public interface, meaning anyone that picks it up can use it. When you enter the passcode, the Firewall authenticates you and the operating system fires up a persona interface for you.

When you engage the persona, several things happen. First, you are immediately assigned an access ID (p. 223, *SR4A*) which stays with you for the duration of your session. This access ID may be spoofed (see p. 232, *SR4A*), but this must be done before you open connections to other nodes; otherwise, the switch in access ID will immediately sever all of your connections. Second, you gain access to all of the privileges your account offers (p. 225, *SR4A*). Third, you gain access to all of the programs and data stored in the device that the account has access privileges too. You may run these programs, loading them into active memory, at which point they count against the node's processor limit (p. 48). Fourth, you are assigned an icon that represents you in AR or VR interactions, which you may modify as you see fit. Fifth, your persona informs your Matrix Service Provider that you are online and that your commcode should be routed towards that particular node and access ID, so that you receive all of your messages and calls.

Other users may use the same node as you, of course, interfacing through their own, separate personas. Programs that they run also count against the node's processor limit, which is why nexi are better equipped for multiple users than standard nodes. (Note that even peripheral nodes have persona interfaces, though these are obviously more limited.) Other personas from the same node will not have the same access ID as you, though all such access IDs will leave a datatrail that leaves back to the same node (and, in particular, a specific account on that node).

From your persona interface, you may access other nodes. If you are simply making a comcall or data request, accessing a public site or profile, or otherwise connecting to a public account, no subscription or login is required—your access ID suffices. If you are logging in to a user/security/admin account, communicating with encryption, controlling an agent/drone, or making some other bandwidth-intensive connection, a subscription is required, and counts against your subscription limit (p. 51). Your activity is logged, creating a datatrail that may be used to track you (p. 55).


knows where to send the answer. Thus both nodes, the sender and the receiver, have to be aware of the other's access ID for a successful data exchange. Every node in between tries to forward the traffic a little further to the receiver. In the wired part of the Matrix, the nodes performing these relay tasks are the routers of the Matrix's backbone.

The wireless part of the Matrix is a decentralized mesh network. This means that every node will work as a router for all the other nodes around it. If a node wants to go online, it just connects to the next available node around it, which in turn is connected to other nodes, and so on, through to the destination. These connection processes are hidden to Matrix users; a persona never "sees" the nodes through which it is routed, nor is there any possibility to log onto the nodes through which a connection is routed.

### Routing

A routing is established every time data from node A want to access node B, facilitating other nodes in between as routers. Due to the mesh-network nature of the Matrix, every wireless node can function as a router and will do so if not in passive or hidden mode (see *Device modes,* p. 223, *SR4A*). Even peripheral nodes participate in the mesh network routing, though priority is given to standard nodes and nexi. A construct is not aware of the nodes it is being routed through and cannot access them. However, a construct can analyze the traffic that is routed through a node (see *Intercept Traffic,* p. 230, *SR4A*).

How does a connection know what route it needs to take? What sequence of nodes it must hop through to reach its destination? Simply put, the node broadcasts a "routing request" which is then passed along by all nodes around it, and so on, leaving backwards pointers at each step along the way, until it reaches the target. The destination then follows the route request trails back, and a connection is established. To help such routing along, backbone infrastructure nexi maintain routing databases.

If for any reason a node or group of nodes is dropped from a network, the remaining available nodes simply route around the gap, making the network self-healing.

### Data Requests

In 2070, most of the traffic through the Matrix is caused by data requests. People want to read their favorite website, watch the morning news, or grab the latest episode of Karl Kombatmage. AR users want to get the profile of the person sitting at the bus station, read the history of an exhibit, or get the price tag of some item. Nodes want to read pieces of data out of databases, synchronize timetables with other nodes, and distribute data. Even phone calls and simsense broadcasts are packaged into requests.

**ACTIONS HANDLED BY DATA REQUESTS:**

- Audio/video communications
- Database access
- File transfers
- Newsfeeds and updates
- Social networking
- Text/graphic messages
- Website requests

Nodes send data requests to the Matrix, and other nodes answer with the needed data package. Most data are protected by access rights, and requests are only granted if the proper access rights conditions are met (see *Accounts,* p. 52).

### Datatrail

Every interaction on the Matrix leaves a record. When a construct or node interacts with another construct or node, even when just routing a connection through the Matrix, access IDs are used in order to identify each different party and avoid confusion and conflicts. These interactions are typically logged, including the access ID. This information may be used to investigate what actions took place (see *The Access Log,* p. 65) or to track down a particular construct to its originating node (see *Trace User,* p. 232, *SR4A*). For this reason, many hackers make efforts to spoof their datatrail (see p. 232, *SR4A*), anonymize their activities (see *Proxy Servers,* p. 104), or edit away incriminating logs (see p. 65).

### Subscriptions

In the case of full AR and VR connections (including the interactive simsense needed by a jumped-in rigger and sensible connections needed to command agents or drones), a simple data request is not enough. In these and other cases (see the Actions Needing Subscriptions table, p. 55), a fast, two-way, maintained connection called a *subscription* is needed (see *Subscriptions,* p. 224, *SR4A*). A persona can only maintain a number of subscriptions equal to the size of its subscription list (System x 2). If more subscriptions are assigned, each additional subscription over the limit counts as an additional program run on the node and may lead to Response degradation (see *Matrix Attributes,* p. 221, *SR4A*). Agents or other constructs run on a persona do not take up a subscription slot. For security reasons, agents (or IC) loaded onto a persona may not be subscribed by other personas. Agents loaded onto other nodes may be commanded as normal.

**ACTIONS NEEDING SUBSCRIPTIONS:**

- Accessing a node*
- Command connections to drones and agents
- Encrypted connections†
- Jumped-in rigger connections to a drone
- Slaved connections (p. 59)
- Tacnets (p. 125)
- Using a program on another node

* An agent run on a persona does not take up an extra slot, while an independent agent does

† Only encrypted connections that wouldn't otherwise take up a subscription slot count. For example, an encrypted link to an agent takes up only 1 subscription, not 2.

## NETWORKS

Not all nodes are directly linked to the world-spanning Matrix. Some are instead gathered in isolated networks, including corporate, national, and private networks. Some networks exist only at certain time intervals, and some are never connected to the Matrix, protected behind wireless-inhibiting walls or other defenses. Some have various access nodes to other networks and grids, while others only have one gateway (see *Chokepoints,* p. 72) that is heavily protected. In principle, anyone with two nodes has the ability to form their own network. The most well-known examples of networks are the PANs that everybody in 2070 carries.

### Grids

Grids are a series of interlocking networks. Every grid is run by one or more Matrix service providers, who maintain the infrastructure of the component networks. Grids are organized into Local Telecommunication Grids (LTGs), used by cities and corporations (and also Private Local Telecommunications Grids, or PLTGs, which are not open to the public), and Regional Telecommunication Grids (RTGs), which connect the LTGs and PLTGs in a given state or nation. The RTGs connect together in a global network to form the Matrix. Space stations like Zurich Orbital also have links to the Matrix, but maintain their own private networks.

## NODE CONFIGURATIONS

Certain node configurations are more useful than the standard network model for security and other purposes.

### Clusters

Sometimes, you have a lot of low-powered devices, but what you really need is a single node able to sustain several personas and/or run a lot of programs at once. For this purpose, two or more nodes can be linked together to work as one super-node or cluster with greater processing power. To do this, all the nodes are linked together and placed into cluster mode, requiring a Computer + Logic (2) Test. Admin access on each node is required for this operation. Once clustered, the group of nodes is treated as a single node with effective Firewall and System ratings equal to the lowest respective ratings of the nodes. The cluster's Response is equal to the average of the node's Response ratings. The processor limit is determined by adding the respective limits of the nodes composing the cluster and halving them. Persona limit is determined by adding the respective limits of the devices together. All accounts present in each node are valid for the cluster node. Agents or other constructs run on a persona does not take up a subscription slot. For security reasons, agents (or IC) loaded onto a persona may not be subscribed by other personas. Agents loaded onto other nodes may be commanded as normal. To avoid conflicts in data routing, the cluster connects to the Matrix as a single node. One node is selected when the cluster is formed and this node provides the access ID for all persona and programs running on the cluster.

### Slaving

One node, the *slave,* may be linked to another node, the *master.* In this setup, the master is given full admin access to the slave. When slaving a node to a master, the slaved node does not accept any Matrix connections from any other node but the master and instantly forwards any connection attempts to the master.

Hackers have three options when faced with a slaved node. First, they can hack in directly to the slave with an additional threshold modifier of +2, though this requires a physical (wired) connection to the device. Second, they can hack the master node (thus gaining access to the slaved node—and any other slaves—as well), though this node is usually more secure. Third, they can spoof the access ID of the master node and then spoof commands to the slave.


## SCULPTING

The Matrix is not real. It is a virtual environment where the user only sees what the node shows her. Behind the scenes, nodes are processing huge amounts of data and performing various tasks that are not visible to the Matrix user. The virtual environment was designed to help users better grasp and process the wealth of available information. Because of this, icons in the Matrix are interchangeable. Depending on the theme or metaphor of a node, a piece of data could look like a piece of paper, a crystal block, a bubble, or even a flying pig. Furthermore, what Matrix users see depends on what they are looking for and what they are doing. Modern Analyze and Browse utilities filter irrelevant information and present the user only icons useful to him. A data search in a node might be represented as a large list of information flying around the icon of the user, while other personas looking at the icon might not be able to see the list, depending on their Analyze program. On top of that, Matrix users are able to use reality filters (see *Reality Filter,* p. 233t, *SR4A*) that override the given theme of a node with their own sculpting.

Every Matrix user has to take the subjectivity of the Matrix into account when he surfs virtual reality. Everything is purely symbolic. It is, for example, not possible to hide behind a large data file that is represented as a big pile of paper. This big pile of paper might appear as a little envelope to another user with a reality filter or might not be visible at all to others.

Though VR sculpture can also be viewed via AR (in a manner more akin to looking through a two-dimensional window than immersing into a three-dimensional environment), this is usually avoided in favor of simple icons and window interfaces.

## METAPHORS

The environment of every node, network, and grid is sculptured according to a certain metaphor. The owner of the grid, network, or node decides what kind of theme to employ and how the substructure of the theme should look to Matrix users. For example, the group that runs the Seattle Matrix decided to give it the famous "Emerald City" metaphor.

A metaphor applies not only to the visual components of the Matrix, but also to all the other senses, especially hearing and smelling. This means that the medieval metaphor of a castle not only incorporates a large virtual castle you can see and walk into, but also includes the sound of birds flying around you and the smell of home-baked bread. One might think that this is merely fancy, useless stuff, but an experienced Matrix user can get information from all of it. The bread, for example, could be a representation of a finished process, the smell reminding the system administrator to initiate another process. The song of the bird could be the alarm of IC that just spotted an intruder, and so forth. In the completely different theme of a high-tech temple, a finished process might be represented by a product materializing in a replicator device straight out of science fiction. The silent alarm of the IC could be a flashing line on the walls of the temple.

However, more than just visual information is governed by the metaphor. The physical laws of a Matrix environment are also shaped by its theme—how heavy things feel, how light bends, what topology a room has, and so forth. You could be in a room that bends back into itself where you arrive at the same place if you just go straight ahead. Or you could be on the surface of a large planet where everything feels twice as heavy. Or you may look into a mirror that does not show everything mirror-inverted.

### Restrictions for Metaphors

Metaphors cannot do everything. A metaphor cannot keep a Matrix user from the task he could normally do. If a user has access rights to a certain file, and the metaphor says that it is in a room without a door, the user will be able to access it anyway by simply beaming there. Such behavior is judged to be very bad coding, and good sculptors and metaphor designers try to avoid such things at all costs. A less severe example is a metaphor that does not allow icons to fly in a locale where they would have to be able to fly to perform some action. This could be as trivial as a piece of data represented by a book standing out of reach high on a shelf. Rather than keep the book from the user, though, the book would just beam into the hand of whoever had the proper access. A final example is the visibility of icons. The metaphor could say that they are completely invisible, very small, or somehow obfuscated. If the persona interface decides the user could easily see them, though, they are replaced by something more visible.

### Icons

Every icon in the Matrix represents data, a construct, a program, or a portal (see *Portals,* p. 58) to a node. There are other objects in the Matrix that do not represent anything other than decoration, but they are not called icons. The tree in front of a

castle could represent a control program governing the climate of a greenhouse under its control, in which case it would be an icon. But it could also simply be a tree put there by the sculptors, an object that does not do anything.

All icons carry an identifying tag, giving the VR user instant knowledge about the kind of icon he is looking at; AR users get a small descriptive tag next to the icon. The kind of information provided depends on the access rights of the Matrix user. In some cases wrong tags may be supplied. While a spider with security access might be informed that the knight's armor in front of him is a trace IC, the hacker with only user privileges might be told that it is only a piece of data. In this case the hacker must use Analyze software to get the complete information.

Additionally, all icons have an access ID attached. Data icons use the ID of the node to which the storage is connected, and constructs and programs alike use the ID of the node that is running them.

### Nodes

In the Matrix, a node can look like a skyscraper, a cornfield, a whole village, an undersea domain, or only one room—the possibilities are endless. Typically a node is represented by a single structure, like a mansion, a ship, or a space station, but even if a node is depicted as a whole conglomerate of houses or a vast realm, the node is still only one node.

In many cases, different functions of a node will be represented as different areas. This is particularly true of nexi, which handle multiple functions and users. For example, a node's files may be represented as a warehouse filled with crates and packages, its wireless functionality as a radio tower, and its security controls by a police station.

No matter how big part of a node's virtual environment might seem, it is important to remember that space does not really exist inside the node. You may have accessed part of a node that is depicted as the top of a major mountain peak, virtual miles away from other parts of the node, but if you Browse for a file or seek to Analyze another user on the node, they will be within sight or reach.

### Networks and Grids

VR representations of networks and grids are mostly a collection of portals to other nodes. A network could be represented as a city, for example, with every building being either an icon, a node, or simply a piece of VR sculpture intended to add detail the virtual environment. Portals to individual nodes or networks (see p. 58) may look completely different than the nodes to which they are connected. By entering a train station, one could suddenly stray upon a vast field, facing a hut, with a city nowhere in sight. Most nodes provide a fitting VR interface to make such transitions between nodes and networks seamless.

### Clusters

The individual nodes that make up a cluster (see *Clusters,* p. 55) normally share the same metaphor. This is not necessary, but the connection of different themes often results in bad coding glitches where the two metaphors meet. Alternately, the cluster may present a single metaphor to each user as they access the cluster, with each sub-node represented as different rooms, buildings, or other partitioned areas featuring their own distinct metaphors.

#### MATRIX PERCEPTION AND TOPOLOGY

The basic use of Matrix Perception in the *SR4A* rulebook allows users to scan an entire node. Users may even set their Analyze program to do this automatically, as noted on p. 228, *SR4A,* and this is certainly a good way of handling security with resident spiders and IC (see p. 69). Some of the advanced topology described in this book, however, has an impact on Matrix Perception.

The large nature of nexi (see p. 196), with processing power and virtual space for large numbers of users, programs, and other icons, makes Matrix Perception more difficult. It simply takes time to process all of the icons and activity in such a busy environment. Divide the processor limit of a nexus by 10 (round normally). This is the number of Combat Turns it takes your Analyze program to complete a full scan of all users and activity in the node. Alternately, if you don't want to take the time to perform a detailed scan, you can make a quick scan and hope you happen to catch what you're looking for. In this case, take a Simple Action to make a Matrix Perception Test with a dice pool modifier equal to the processor limit ÷ 10 (rounded normally).

If two nodes are slaved together (see *Slaving,* p. 55), icons in one node can choose to make a Matrix Perception Test on the other node, as if they were in that node, due to the nature of the connection. Only one node may be scanned at a time, however, they may not be scanned together.

In the case of a node cluster (p. 55), the entire group of nodes is considered to be a single node for Matrix Perception Tests.

### Reality Filters

Reality filters (see *Reality Filter,* p. 233, *SR4A*) help a user obtain more information out of the virtual environment he experiences. Though most metaphors try to provide a Matrix user with the best information experience possible, it still takes some time to get used to a certain theme. In principle, the reality filter is a huge library that relates icons with certain shapes and forms, overriding the VR information from the icon itself. A hacker running a reality filter with a science-fiction theme might see an attacking IC as a combat robot, while it was a knight in shining armor in the original medieval metaphor of the node. Depending on the complexity of the environment and the quality of the reality filter, it helps the user to adapt more quickly to the environment of a node.

## VIRTUAL TOPOLOGY

The virtual topology of a network or grid does not need to be connected in any way to the hardware's setup in the real world. Two nodes might seem to be right next to each other in the Matrix while they are many miles apart in the real world. The

Matrix topology is shaped by the networks and grids along with the protocols used for connecting different nodes.

### Movement

When a persona accesses a node, in VR it will enter the node and be inside the virtual environment. If the persona is accessing multiple nodes at once, it will seem to be in one node at a time, though it can easily switch between them like changing a channel, and it can also keep track of the environment of other nodes via virtual window interfaces.

The persona's datatrail, connecting the node from which it accessed the Matrix (and which runs its persona and programs) to the accessed node, might be routed through dozens of nodes via wireless connections and/or fiberoptic cables. The persona is not aware of the nodes through which it is routed, however—it can neither see nor access them. As a consequence, a persona only experiences movement inside a node. The transition between nodes is instant, though Matrix metaphors might visualize this in many different ways (doorways, slides, space warps, etc.). Inside a node, the movement is also governed by the theme of a node.

### Portals

The VR environment of a node might contain a portal to another node. Does this mean that one can only go from this node through the portal to the other node? Far from it. With the exception of chokepoints (see *Chokepoints,* p. 72), a Matrix user can connect to any node for which he possesses an access ID, as long as that node is online and/or within Signal range. Public node access IDs are easily located via search engines, secured nodes may require some legwork to uncover.

A portal is simply an icon that represents the access ID to another node. By going through that portal, the construct accesses the node the ID is related to. Just like any other icon, portals are subject to the metaphor of the node and can look like anything: a door, a bridge, a hole in the ground, a beaming station, or a taxi that drives users to another node. The admin of a node can choose to implement as many portals in the VR environment as he wishes.

## PAN TOPOLOGY

To regular Matrix users, and especially shadowrunners, what matters even more than Matrix topology is the topology of their personal area network (PAN; see *Networking,* p. 221, *SR4A*). The manner in which a runner organizes, connects, and secures his devices can mean the difference between life and death.

At the core of every personal area network is the *person.* The user accesses and controls this network through his persona, usually via commlink, though other devices maybe used.

## INTERFACE

You can choose one of two methods to physically interface with your commlink (or any other device, for that matter): you can use your brain (direct neural interface), or you can use your body (manual).

### Manual

Using your body is as simple as picking up your commlink and accessing the physical controls. In the 2070s, however, this is a horribly inefficient way of doing things. In game terms, manual use of a device takes a Simple Action (see *Use Simple Object,* p. 148, *SR4A*). Most devices have physical controls for their basic functions (on/off, mode, volume, etc.), and some devices will offer holographic menus and controls (monitoring where in the holo you touch for input). Most will also respond to verbal commands from an authorized user. If you want advanced features, however, you need to access their controls via augmented reality.

Even without a neural interface, you can access augmented reality, but you have to use special equipment such as goggles or contacts with a display link, earbuds, AR gloves, feedback clothing, and so on (see *Augmented Reality,* p. 219, *SR4A*). Each of these items allows you to physically sense AR data with your body (rather than directly with your brain). They also allow you to interact with AR by sensing your physical response. For example, the accelerometer in AR gloves measures your hand movements, and AR goggles detect your eye movements, so you can use your eyes like a mouse and blink to click.

If you wish to make commcalls, you must wear a microphone or use the built-in mic on your commlink, like a cellphone. You can make video/trideo calls using the commlink's camera, or simply display your persona icon to callers.

### Direct Neural Interface

Using your brain requires either a cybernetic implant or the use of trodes. Either counts as a direct neural interface (DNI), meaning that it can send and receive signals directly to and from the brain. Such components include software that interprets signals in the brain and translates them into instructions that devices or software environments understand, and vice versa. This means that you can control and access devices at the speed of thought. In game terms, DNI use of a device is often a Free Action (*Changed Linked Device Mode,* p. 146, *SR4A*).

You can exercise DNI control over any device you have an electronic link to. If your commlink is plugged into your datajack via fiberoptic cord, you can mentally control it. If your smartgun is wirelessly linked to your smartgun implant, you can control that via DNI as well.

When you mentally access a device, your interaction with that device literally takes place in your head. You simply *think* to talk to someone over a comcall, access a menu, call up a diagnostic, or execute a command. The device sends information that is translated by the DNI interface into something you can understand, though such mental input is somewhat different from physical sensory input. Seeing something in your mind's eye, for example, is not quite the same as *seeing* it physically. For this reason, many users still make use of display links and the like. In fact, integrating manual components with a DNI-controlled PAN is not uncommon.

### Simsense

While DNI is fast and useful, the standard DNI interface is not equipped to translate simsense signals. For the brain to be able to understand simsense signals (and thus access virtual reality; see p. 225, *SR4A*) a sim module is required. Whenever a user is interacting with a virtual environment, all communication between the brain and commlink is routed through the sim module, which converts them into machine code for the commlink and sim signals for the brain.

Simsense can also be used for experiencing AR. In this case, a partial simsense feed is applied, allowing the user to experience AR sensory input directly in their brain via sim signals. This makes a commlink with sim module the perfect combo package for experiencing AR and VR and interfacing with devices via DNI and simsense—no other gear required.

## PAN HARDWARE

What items compose the components of a PAN? This is up to each particular character, but the general rule is that any computerized electronic device carried by the character counts.

### Commlink

The commlink is the so-called "hub" of the PAN. As a standard node with the best Signal rating (usually), it acts as the primary routing device in the network. It is also the device that the user directly accesses and engages their persona, and from which they make calls, send messages, and access other nodes. For more details, see *Networking,* p. 221, *SR4A.*

By taking on the role of hub, the commlink can be used to keep track of all of the other devices in the PAN. This is usually accomplished by giving the character's account on the commlink an equivalent node account (see p. 52) on each device. This grants the character access privileges on each sub-node without having to log in, and makes it easier for the character to access data from each device. This means that a character logging into his persona can, for example, automatically check the ammo level in his gun, the remaining power in his drone's fuel cell, the stock levels on his medkit, and the credit left on his credstick. The commlink can also be sent to immediately notify the persona if a device disappears from the network (a handy way to keep from leaving things behind). The drawback to this, of course, is that if that particular commlink account is hacked, all of the devices in the PAN are compromised.

### Sub-Nodes

The rest of the PAN typically consists of other devices with computerized components—which in the 2070s is almost everything: weapons, clothing, drones, vehicles, other electronics, RFID tags, credsticks, cybernetic implants, and other gear. Most of these items are peripheral nodes (p. 48) with limited capabilities, with the exception of items like drones and vehicles.

While many of these devices have a low Signal rating anyway (and so don't mesh with other nodes much), it is common practice to keep all of these items in hidden mode, only communicating with the commlink. Not only is this polite (less wireless "traffic clutter"), it is also prevents someone from compiling a sneak inventory of what you are carrying and makes these sub-nodes less tempting targets for hackers. If the sub-node needs to communicate with a node external to the PAN, the connection is simply routed through the commlink.

### Decoy Commlink

Many runners prefer to carry a decoy commlink which they run in active or passive mode, accepting commcalls, and store their fake ID and credentials on. Their real—and more secure—commlink is kept in hidden mode, and serves as the PAN hub. Though this has many advantages, it does mean that the character must switch back and forth between their decoy commlink and their real one as the situation demands.

## PAN CONNECTIONS AND PROTOCOLS

The manner in which the PAN components are connected plays a crucial part in PAN security. Note that each device does not need to be connected to every other device in the network, as long as there is a chain of connections leading to other devices (i.e., the PAN is also a mesh network).

### Wireless Links

The most common method for each node in a PAN to communicate with the rest is via radio. The Signal rating (p. 221, *SR4A*) determines its range and power. The advantage to wireless is that you don't have to deal with cables and things can be moved around easily, as long as they stay in range. The drawback is that wireless signals can be detected, intercepted, jammed, and spoofed (see *Matrix Actions,* p. 228, *SR4A*).

### Wired Links

A less practical but more secure option is to use fiberoptic cable to connect devices. The obvious drawback is that this limits your range and cables can get tangled and in your way. The advantage is that wired connections cannot be jammed. In order to intercept a wired connection, a hacker would need access to one of the wired devices (see *Intercept Traffic,* p. 230, *SR4A*). For this reason, many hackers use a fiberoptic cable to link to their commlink via trodes or datajack.

### Skinlink

A third option is to use skinlink (p. 328, *SR4A*), where a connection is established using the skin's electrical field. For a skinlink connection to work, both devices must be touching the skin (or close to it—the electrical field extends a bit beyond the skin, so clothing does not interfere), and both must be equipped with the skinlink accessory. Cybernetic implants may also be equipped with skinlink, even if they are not accessible on the body's exterior—in this case, a simple connection is established between the implant and the skin's surface.

### Slaving

Perhaps the easiest way to secure a PAN is to slave each sub-node to the commlink (see *Slaving,* p. 55). This will automatically forward any wireless connection attempts on a slaved sub-node to the master commlink. In order to hack a slaved device, the hacker will either need to hack the more secure commlink or gain physical access to the item.

### Clustering

If you lack a commlink or other standard node, you can cluster a number of peripheral nodes together so that they act as a single, unified node (see *Clustering,* p. 55).

### Encryption

Another good line of defense for your PAN is to use encryption. You can encrypt your wireless transmission, your node, and even your files, forcing a hacker to chew his way through scrambled code to get what he wants (see *Encryption,* p. 65).


The dragon is bored.

As she steps through yet another doorway made of rice paper and a richly dark wood, her eyes settle on a scene that would awe any other person. Before her stretches a beautiful garden, surrounded by groves of trees. Stone bridges arch artfully across arranged water features, while small creatures rustle their way through a lush array of flowers, ferns, and other plant life. To the dragon, it is possibly the dullest thing she's ever seen. Uncoiling her digital scales, the emerald green dracoform rises, floating above the imagery of nature tamed.

She catalogs the symbols as she glides past them. A heron wading through the datastream river is a piece of noisy alarm software. A raccoon snuffling for food beneath a bush is a trace program. The dragon inclines her head to look down at a large statue of a samurai, its blade outstretched, a particularly nasty intrusion countermeasure intended to slice and dice anything the other software doesn't like.

As the great dragon moves from one node to the next, she notes a change. Her commlink filters the signal as a scent on the air, a pungent musk that tells her that something is out of place. Diving toward the ground, the creature's emerald scales shift, blending into the rich color of a bed of ferns near an ornate teahouse.

There is another user in the system, a user that has absolutely no reason to be here. Even now he is showing the Kitsune® program a virtual ID. The dragon can smell it, even from where she is hiding. Hacking. Fakery. She sidles around the building to get a better view of what the man is doing.

The man, little more than a dark silhouette in a suit, has just settled down to work the controls set into a table in the middle of the teahouse. His fingers spin across the readings and coolly press buttons with the ease of a pro. The Kitsune® has not disengaged, the small fox-man stands staring at the suited visitor. Something about the user's badge has tipped the software. The dragon snorts: this man is an amateur.

Amateur or not, he is about to disable some sensitive safety equipment in one of the lab's most secure areas. The dragon rears a bit, and flexes her ears. All around her, she feels the lush setting changing to suit her whims. Programs across the system are now active, and none of them servile to any but her. Before her eyes, the Kitsune® becomes more alert. It seems to realize its earlier mistake and leaps at the hacker's exposed back. Leaning out of the underbrush, the dragon aids the fox-man by calmly biting off the man's head.

Spraying bits and bytes, the man's form slumps to the ground, dissolving into digital symbols slipping between wooden slats. Wary, the dragon looks around the teahouse again. The Kitsune® bows low to the security hacker and fades away. The dragon nods, satisfied.

Boring, the garden may be. But the garden is still hers.


IDENTIFICATION
ORDER NO. 1219
WANTED
UNIDENTIFIED
HACKER
DIVISION OF INVESTIGATION
DEPARTMENT OF JUSTICE
Fingerprint Classification
DESCRIPTION
CRIMINAL RECORD
RETINA SCAN:
PROCESSING DATA
SECURITY

A chain is only as strong as its weakest link. This goes doubly for computer systems, which can be attacked at three points: the physical device, the virtual node, and the legitimate user. A hacker only needs to find a single chink in the armor to completely take over a system. This chapter discusses principles and practices by which a system can be secured, from the lowliest PAN to the greatest nexus.

# PHYSICAL SECURITY

An attacker that can reach the physical device of a system has more power over that device than a hacker trying to reach it via the Matrix. Keeping an attacker out is more than just guards and cameras. There are a number of physical practices that a facility can use to help bolster its Matrix defenses.

## PHYSICAL FACILITIES

The physical security of a facility is necessary to protect the integrity of any Matrix system housed there. Most physical security can be handled by established techniques (*Security Systems*, p. 259, *SR4A*). There are more specific measures that can be taken with regard to Matrix security.

### Landscaping for Signal Attenuation

When all of your devices are wireless, it is important to take steps to keep the signal from leaking too far from a controlled area. Proper landscaping can create greater attenuation, or signal loss, than would otherwise be present. Hills and other earthen features usually contain compounds of iron or other metals, which cause attenuation and reduce effective Signal ratings by 2 to 5 per meter of thickness, depending on metallic content.

Water also causes rapid attenuation, especially salt water. Every 10 cm of fresh water and every 1 cm of salt water reduces the effective Signal of a device by 1. Flora also reduces the effective Signal of devices, mostly because of the water held in plants. For every ten meters of foliage or five meters of dense foliage, reduce Signal ratings by 1.

### Wireless Negation

Wireless negation (p. 264, *SR4A*) is a highly useful tool that absorbs some of the wireless signals coming from either side of the surface it covers. It is available as both wallpaper and paint in several different colors and textures, all with a dull, dead look that is despised by decorators and artists.

Faraday cages are a more extreme form of wireless negation. A Faraday cage is an enclosed structure made entirely of a conductive material, usually metal. The walls of a Faraday cage may be solid or take the form of a narrow mesh. When the cage is closed and electromagnetic waves hit the outside (or inside) of the cage, the energy from the wave is dispersed across the surface of the outside (or inside) of the cage. In practical terms, a Faraday cage prevents wireless signals and other electromagnetic waves (as from HERF guns or EMP effects) from penetrating either from the outside or the inside.

### Telematics Infrastructure

Telematics Infrastructure (TI, pronounced "tie") is a tracking system for vehicles, drones, and personnel. It works via a network of TI programs running on individual commlinks, devices, and even RFID tags. It combines sensor data, GPS information, and wireless scanning to detect and track all individuals within its boundaries and report anomalies.

TI will automatically detect and report any wireless device in Active or Passive mode that enters its coverage area. Various parts of the network also scan for Hidden nodes; use the rules for Detecting Wireless Nodes as an Extended Test (p. 230, *SR4A*) except that the TI system makes only (Rating) rolls per minute and scans its entire coverage area.

The information generated by the TI network can be fed to a TacNet (p. 125) or any other user or device that is "TI'd into the system." This information includes the position, direction, and speed of any wireless device within the coverage area, along with its access ID and any public data offered by the device.

## ACCESSIBILITY

Another way to keep a system secure is to simply keep people from getting to it. This is more difficult in a wireless world, especially when more and more people are finding the thought of office professionals with datajacks in their heads to be quaint. Still, there are effective ways to increase security without losing utility.

### Cabling

One of the ways to escape the hazards of wireless networking is to take the wireless out of the network. Devices that have their wireless capability disabled can be connected via fiber optic cables. These cables have the advantage of being invulnerable to wireless attack, although it removes the ability to move devices or to easily replace them.

Another consideration is the ubiquity of wireless among the users of a facility. Employees, customers, soldiers, and other personnel will very likely have their own commlinks, and expect to work with the system via wireless AR or VR. Training personnel that expect to be able to walk into a room and use its systems

| Wireless Negation | Availability | Cost |
|---|---|---|
| Wireless Negating Paint, per can (30 $m^2$ coverage) | Rating | Rating x 20¥ |
| Wireless Negating Wallpaper, per 10 $m^2$ strip | Rating | Rating x 5¥ |
| Faraday Cage, per $m^3$ | 4 | 100¥ |

| Telematics Infrastructure Software | Availability | Cost |
|---|---|---|
| Telematics Infrastructure (Rating 1–3) | (Rating x 2)R | Rating x 400¥ |
| Telematics Infrastructure (Rating 4–6) | (Rating x 2)R | Rating x 800¥ |

with their image links is an expense that many corporations, governments, and other entities see as unnecessary. Some facilities compromise with systems that are cabled except in wireless "safe rooms" protected by wireless negation.

### Traffic and Access

The physical location of the devices in a system is another important security concern. Some placements are obvious: cameras should be placed at entrances, locks are installed into doors, etc. Standard nodes and nexi, on the other hand, can be placed almost anywhere, especially in a wireless environment. It is important, therefore, to give proper consideration to the placement of such devices, to deny physical access to any person that does not need to have access to them. By the same token, they should be kept away from the main flow of physical traffic in which most personnel work or travel.

## SECURITY NETWORKS AND RIGGING

A facility's physical defenses can be effective on their own, with autonomous devices and security sensors, but when combined with a security specialist, or spider, they can keep out all but the most tenacious intruder. The various security devices in a facility are joined together by one or more hub nodes into a security network, which is overseen by spiders. This section discusses security networks in practice; more information about the spiders that use this practice can be found later in this chapter.

### The Security Network

A security network is simply a network of devices that are assigned security roles. These devices usually include cameras and other sensors, locks, automated doors, drones, and automated systems such as gun emplacements or containment systems. Anything with a Device, System, or Pilot rating can be integrated into a security network, including agents, IC, and even the smartguns and cybereyes of security guards.

These devices are then linked or slaved to one or more security hubs. A security hub is simply a device that acts as a focal point for command and control of the network. It can be a standard node or a nexus, or even a commlink. The spider on duty monitors the hub, and often uses it to run his persona. Any device or icon that is linked or slaved to the network is considered linked to all other devices in the network.

In large installations, it is not uncommon to find multiple security hubs dividing the security. In some networks, the split is geographical, with different hubs controlling different areas of a facility. In others, the hubs are assigned to different types of security, with one hub handling drones, another handling locks and doors, another dealing with security personnel, and so forth.

Security networks do not need to be installed in a permanent facility. They are installed in vehicles like semi-trailers, aircraft, and naval vessels. Security networks do not need to have physical bounds, and are found protecting police squads, military fire teams, and even shadowrunning groups.

### Information Operations

The most basic function of a security network is to allow a spider to observe a large area from a single location. Devices in a security network send a constant stream of real-time data to the hub node, or to multiple hub nodes. Should a device detect a status change (e.g. a camera sees movement, a weapon is fired, a program in a node starts or stops, etc.), it automatically notifies the spider using a Free Action. The spider can then use the Observe in Detail action (p. 147, *SR4A*) to investigate using the data feed from the specific device.

### Remote Command and Control

A security network allows a spider to do more than merely observe. A spider is empowered by her security network to take indirect or direct action against intruders and other security threats. The simplest way this is accomplished is through command and control, using the network to communicate orders and information. The spider can use the Issue Command action (p. 229, *SR4A*) to send instructions to any automated device on the network. She may also use the Speak/Text Phrase action (p. 146, *SR4A*) to direct security personnel, or if more detail is necessary, she can use the Transfer Data action (p. 229, *SR4A*) to send a full situation report and orders.

Another option for the spider is to use the Command program to control a subscribed device on the network (see *Control Devices,* p. 229, *SR4A*). This can be done in AR or VR, and does not require any form of simsense. This option allows the spider to address a security breach in conventional ways, such as by firing an automated gun or controlling a drone, or unusual and creative ways, such as opening a door in an intruder's face, changing the temperature in a room, or using the lights to flash a message in Morse code.

A spider using VR can also jump into any device fitted with a rigger adaptation (p. 348, *SR4A*). In most security networks, this is limited to drones. Some more creative security engineers add rigger adaptation to other devices, such as sensors, gun emplacements, and repair or medical facilities. It is possible to add a rigger adaptation to other devices, such as automated doors and windows, locks, and vending machines, but the utility of such a modification is rarely very great.

For more info, see *A Note on Commanding Devices,* p. 104.

# MATRIX SECURITY

While the physical arrangement around a system is important to its security, most of the action happens in the Matrix. Security personnel called spiders act as hackers and/or riggers from within the system, guarding it against intrusion. Intrusion countermeasures (IC) are run on nodes to guard them from attackers, or to mount their own attack against trespassing hackers. Even the very shape of the system's virtual layout can aid in its defense.

## AUTHENTICATION

The first line of security is authentication, the process by which a system determines whether the claimed identity of a user is genuine. The node must be reasonably certain that a user is who he says he is, and is therefore entitled to the account privileges listed for that user.

There are several different ways for a system to authenticate a user. Some are more reliable and secure than others, although for the most part, the more secure an authentication method, the higher its overhead costs.

### Access ID

A system can allow access simply by the access ID of a user. The node keeps a list of access IDs, and any construct that attempts to log onto the node from an access ID on its list is allowed to do so. This is a fast method of authentication, if not a secure one, and requires only a Simple Action to log on with AR, or a Free Action with VR.

This method is used by inconsequential utilitarian nodes, such as garage door openers, public forums, and home appliances.

### Web of Trust

A web of trust determines the authenticity of a user by checking a number of other sources. Data about a user is stored in many places, making it more difficult to fake authentication. To use an analogy, the system asks around to see if the user is trustworthy. This is the method used by SIN verification systems to check a person's ID; in most cases, systems that use this method of authentication use a SIN verification. Treat the authenticating node as having a SIN verification system with a rating equal to its System (p. 267, *SR4A*).

Nodes that use the web of trust method of authentication tend to be public or mostly public nodes, such as municipal or corporate residential libraries, shopping malls, vending machines, and virtual night clubs.

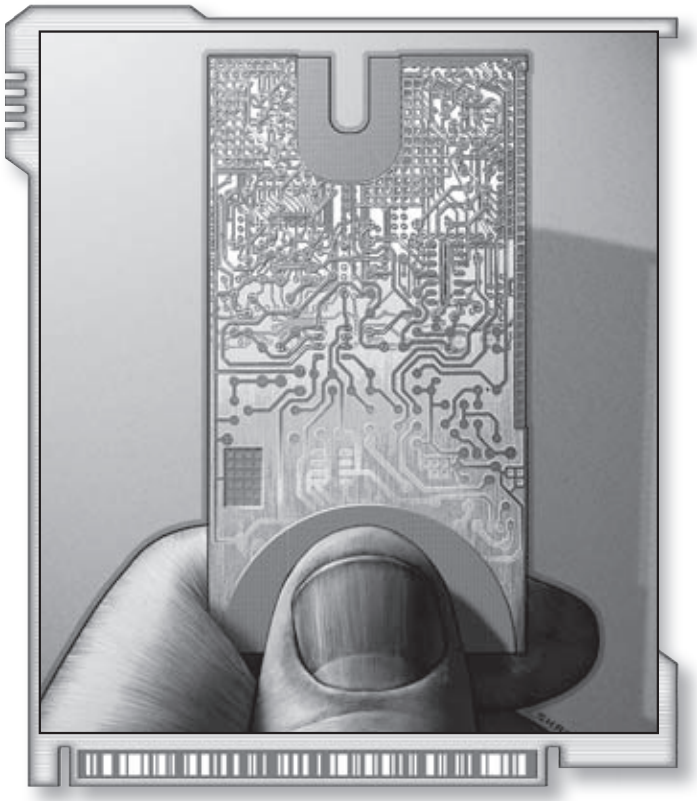
### Passcodes and Linked Passcodes

Passcodes are described on p. 225, *SR4A.* They are the most basic form of authentication, even when linked to additional data. Private and low-security nodes such as private clubs, retail outlets, and public schools tend to use passcodes. Small businesses, local government offices, underworld syndicates, and upper-class homes generally use linked passcodes.

### Passkeys

Passkeys are also described on p. 225, *SR4A.* They are physical modules ranging in size from a fingernail to a stylus or credit card. They use a combination of encryption and materials engineering to create a unique key that is plugged into a common commlink jack. If the correct passkey is not connected to a device that tries to access the node using this method, the access is denied.

In addition to standard passkeys, more advanced passkeys have recently been developed. One of these passkeys is the *nanotech passkey,* in which a small colony of nanites form unique and dynamic patterns for authentication. These passkeys require a small amount of upkeep to sustain the nanomachines, which is usually accomplished by leaving the passkey plugged into a commlink for a few minutes each day.



The second type of advanced passkey is the *alchemical passkey.* This piece of manatech is similar to a magical focus that interacts with technological sensors in the passkey to produce a unique signature. An alchemical passkey is created through a process of Enchanting using different reagents in a process similar to magical compounds (p. 82, *Street Magic*). It has an aura that is recognizable as being magical in nature, but no astral presence.

The passkey is not the only part of a passkey system. The node secured by passkey must also have the proper hardware to use passkey authentication. Such systems are expensive and, in the case of more advanced passkey systems, difficult to maintain, to the delight of hackers everywhere.

No matter what kind of passkey is used, systems that utilize passkeys do not merely check for proper authorization on initial entry into the system. The passkey information is registered with every action in the node's access log. This makes hacking into such nodes far more difficult if the session lasts longer than the next access log update; the hacker is detected and an active alert initiated when the access log shows that the hacker lacks the passkey data.

| Passkey | Cost |
|---|---|
| Standard Passkey | 100¥ |
| Nanotech Passkey | 1,200¥ |
| Alchemical Passkey | 2,100¥ |
| Standard Passkey System | 15,000¥ |
| Nanotech Passkey System | 32,000¥ |
| Alchemical Passkey System | 110,000¥ |

To avoid detection, the hacker can edit the access log to hide the discrepancy. The use (or lack thereof) of a passkey that matches the passkey system on a node can also be detected by a security hacker who has access to the passkey system with a successful Matrix Perception Test.

Fortunately, passkeys are required for access on only the most secure systems. Many facilities do not have the budget for passkeys on every node, and so many only have one passkey node, often used as a gateway to other nodes on the system. Examples of systems that generally use passkeys for authentication include megacorps, federal governments, financial institutions, and military facilities.

### Other Authentication Methods

Nodes may be configured with other forms of authentication. Such methods are usually unique and challenge a prospective user. For example, a node may require that a construct beat it in a game of chess, achieve a certain score in a video game, or pass an intelligence test. If the node is linked to various input devices, it can also demand a certain sequence of movements, or that a user perform a karaoke song correctly.

These sorts of nodes sometimes also challenge users that have successfully logged into the system, with IC confronting constructs with tests and trials that must be answered or an alert will be initiated. Some hackers are delighted by these sorts of nodes, some just hack their way around them.

### Hacking and Authentication

When a character hacks into a node, whether on the fly or by probing, she is actually circumventing normal authentication routines and setting up a fake account that the system believes has access at the privilege level the hacker chose at the start of the attempt. This account is almost never perfect, but the node accepts it as legitimate. Patrolling IC or spiders can discover the forgery by making a Matrix Perception Test against the hacker. The Stealth program helps counteract such snooping, but a hacker cannot expect to be able to use a hacked account indefinitely (see *Account Privileges,* p. 52).

## THE ACCESS LOG

Every node keeps an access log as part of its routine operation. The access log is a file that stores the record of everything done by, in, or to that node. For all Matrix actions performed in a node, records are created. These records include the time and date of each action, the access path of the user or agent that performed it, the account to which the user or agent had access, and the program that was used to perform it. The exceptions to this are Log Off and Jack Out actions (p. 229, *SR4A*), which are recorded with only the time and date of the action, but no access path or data trail information.

Nodes with higher System ratings tend to host more actions and so have larger access logs. The access log is updated automatically by the operating system. Because the operating system of a node has a certain amount of processing overhead, the access log is not updated immediately, leaving a certain amount of "breathing room" for hackers. A hacker's actions will not evident in the access log of a node for at least a number of Combat Turns equal to the System of the node; the information is there, but it is in the form of raw data, and has not yet been processed into a readable format.

Spiders use the access log regularly in their work. Most often, they use it to monitor and verify legitimate access and users. The access log also holds the evidence of unauthorized intrusion that can be read by spiders or agents. Spiders also routinely use the access log after an intrusion to identify and patch weaknesses in the system.

A spider can use the information in the access log to Track an intruder through the Matrix (p. 232, *SR4A*) even if the intruder's icon is no longer in the node. Unfortunately for the spider, hackers tend to change both their location and their access ID on a regular basis, so this information is usually dated and no longer accurate. A successful Track Test using access log information will only give the location from which the hacker performed the last action recorded in the access log, and the access ID that she used at the time.

The access log is also a file of great interest to attacking hackers. To an intruder, the access log is the metaphorical set of fingerprints that betray the hacker's entry into the system. A good hacker will always perform a Data Search through the file and then an Edit to remove any trace of her presence. If she is in a hurry, she may simply delete the file, but such ham-fisted tactics are a dead giveaway that an intrusion happened. Unless the intruder can figure out a way to delete it, her Log Out or Jack Out action will remain behind, leaving evidence of the incursion but no information on who accomplished it or what was done.

An access log can also be encrypted, slowing attacks on it. In order to do this, a node must be running a dedicated Encrypt program to handle both access log updates and the encryption of that data. If the dedicated Encrypt program is deactivated or crashes, the access log is automatically unencrypted. Due to the constantly-changing nature of the access log, it cannot be bundled with IC or a Data Bomb when it is encrypted (see *Encryption,* below).

As a focal point of interest to both attackers and defenders, the access log is a part of many Matrix strategies, both offensive and defensive. For defensive strategies, see *Tips and Tricks,* p. 72, below. For strategies for hackers, see the *Hacker's Handbook,* p. 80.

## ENCRYPTION

Encryption renders data unreadable to those who do not have the encryption key or cannot use Decrypt. It can be used to protect files, lines of communication, and even entire nodes. In *Shadowrun,* the rules for encryption include encoding, ciphers, and other forms of cryptography.

Unfortunately, in the 2070s, encryption is not a very strong protection against prying eyes. Cryptanalysis techniques are far advanced of encryption theory. At best, encryption can only slow down a dedicated attacker. Even so, in a Matrix that moves at the speed of light, every microsecond counts.

All encryption has a rating, which is used to determine how difficult it is to break. The higher the rating, the better the encryption. Usually, the rating of the Encrypt program used is the rating of the encryption. When encryption is initiated, the user selects a key, which may be a word, phrase, ARO, gesture, song, etc. Thereafter, any other user with that key may decrypt the signal, file, or node with a Simple Action.

### Signals Encryption

A connection between two nodes can be encrypted to help protect it from eavesdropping. To make this happen, at least one

Urgent Message...

**OPTIONAL RULE: DRAMATIC ENCRYPTION**

As a gamemaster, you may wish to use an encrypted file or node as a story hook or a plot device. With the state of cryptography what it is in the 2070s, encryption presents a very low bar for players.

Fortunately, there exist unique and particularly arcane encryption methods that represent either bleeding-edge research or ancient techniques that cannot be easily cracked by computers. These methods can only be decrypted under special circumstances, such as only in a certain place, using information from a particular object, only after finding all parts of a file, or simply after an inordinate amount of time. The details of such methods, including availability and frequency, are determined by the gamemaster.

side of the link must be running Encrypt. There is no advantage if both connected nodes are running Encrypt, except that the highest rating of the two programs is used. Initiating signals encryption requires a Simple Action by each node, but no further action is needed to encrypt or decrypt data sent along the link until the encryption is disabled or the link is severed. Encrypted connections take up a subscription slot (see *Subscriptions,* p. 55).

### File Encryption

Files can be encrypted with a Simple Action, using the Encrypt program. When encrypting a file, a user may include more than one file, to create a single encrypted archive file containing several smaller files.

A user may also include a Data Bomb program within the archive file. When doing so, the user also determines the conditions by which the Data Bomb will not activate (usually when it is decrypted using the key rather than by use of Decrypt) and whether or not the Data Bomb will destroy some, all, or none of the files within the encrypted archive. An encrypted archive may contain only one Data Bomb. See *Data Bomb,* p. 233, *SR4A*.

Additionally, a user may include an IC program (which may in turn be loaded with other programs) in an encrypted archive file. During this process, the user configures the IC's behavior when the archive is decrypted, usually including a clause that keeps the IC from activating if the proper key is used. Barring instructions to the contrary, the included IC automatically loads into the node in which the archive file is decrypted. Only one IC program may be included in an archive file.

The presence of a Data Bomb or IC can be detected with a successful Matrix Perception Test performed on the archive file.

### Node Encryption

An entire node can be encrypted as an extra layer of security. An encrypted node can normally only be accessed by a user that has the correct key. A hacker may Decrypt the node, after which she can access it, as can anyone else with whom she shares the Decrypted key. The node must have an Encrypt program running, which counts against its program count for Response reduction. Encrypting a node does not automatically also encrypt subscriptions to or from it or files within it. Encrypting a node requires a Simple Action.

### Strong Encryption

While cryptanalysis is far stronger than encryption these days, it is possible to slow down an attacker more than standard encryption can. Doing so takes a large amount of processing power and time, and is considered by some hackers to be not worth the extra effort.

When using strong encryption, the user needs the Encrypt program, as with normal encryption. The amount of time taken to perform the strong encryption then becomes the interval for an attacker's Decryption Extended Test (p. 230, *SR4A*). The longest period to which the interval may be increased is one day; beyond twenty-four hours, the encryption suffers from dramatic diminishing returns.

Strong encryption may not be used for signals encryption.

### Dynamic Encryption

It is possible to perform continuous re-encryption by monitoring a decryption attempt and adjusting the encryption algorithm accordingly. Doing so does not make the encryption safe, but it can delay an attacking hacker. Like strong encryption, dynamic encryption takes extra time and processing power. It has the additional disadvantage that it requires awareness of an attacker for it to be effective.

Dynamic encryption is only effective against an attacker that has been detected with a Matrix Perception Test and that is currently decrypting a link, file, or node. The user makes an Opposed Computer + Encrypt Test against the attacker's Electronic Warfare + Decrypt; for every net hit on this test, the threshold for the attacker's attempt to break the encryption is increased by one. This requires a Complex Action.

The extra threshold applies only to the attacker against which it is directed. The attacker may clear the threshold penalty by restarting his decryption attempt, but this causes him to lose any hits already accumulated against the encryption.

Once an attacker has fully decrypted a subscription, node, or file, this technique may no longer be used. Dynamic encryption is not compatible with strong encryption.

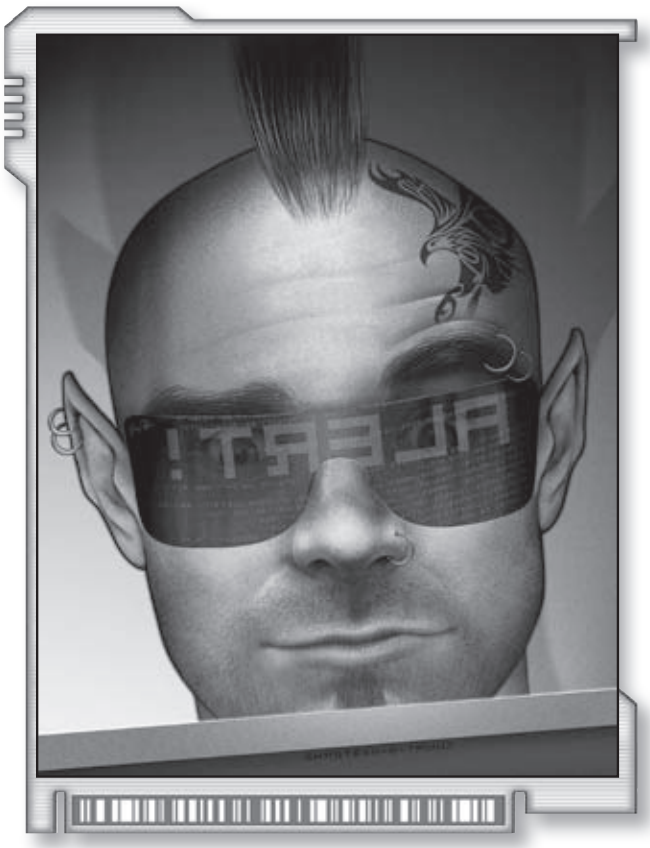
### Decryption

Most of the time, encrypted subscriptions, files, and nodes are decrypted with a key. Often they are decrypted by hackers who crack the encryption with the Decrypt program. Using the Decrypt program requires a Complex Action to start the process, but thereafter the program continues the Extended Test (p. 230, *SR4A*) autonomously. Once a file is decrypted by any user, it remains decrypted, but when a subscription or node is decrypted by a user, it remains decrypted only for that user. However, the encryption may be re-instated under certain circumstances:

Signals encryption may be restored by closing the subscription (a Log Off action), re-establishing the subscription (a Log On action), and then re-encrypting the subscription (a Simple Action from each side of the link).

File encryption is restored merely by encrypting the now-decrypted file.

Node encryption is restored by rebooting the node (a Complex Action, plus boot time), and re-encrypting it (a Simple Action).



## ALERTS

Another important line of defense in any system is the intruder alert. A node under an active alert is "aware" of a specific access ID that has hacked or is trying to hack his way into the system. If a system is made up of multiple nodes, an alert in one node puts all nodes on alert against the same intruder.

A node on alert gains a +4 bonus to its Firewall against the intruder specified in the alert. Additionally, all privileges involving the node itself (such as deactivating programs or agents, rebooting, editing files, etc.) are no longer automatically allowed to the trespasser, who must either use the Hacking skill to perform such actions or Spoof a command from a legitimate user that still has her permissions intact.

> *The young hacker, /dev/grrl, has hacked herself an admin account, but she glitches on a roll and an active alert ensues. While she normally would have been able to Edit the node's access log without rolling, she now must make an Opposed Hacking + Edit Test against the node's Firewall + System to do so.*

An alert is most often automatically triggered by a node's Firewall. Additionally, any user, agent, or IC with a security or admin account may initiate an alert against an intruder with a Free Action. When an alert is triggered, a node executes its alert response configuration (see below).

### Alert Response Configuration

One of the most important duties of the spider is configuring the script that a node automatically runs when an active alert is initiated. The script is called the alert response configuration (ARC). The ARC is automatically executed the moment the alert is triggered. Unfortunately for the spider, the response a node can offer on its own is limited; system software is not designed to handle intrusion, and relies on spiders and IC. A node will execute its ARC only once per active alert triggered, and it will only run it against the icon that triggered the alert.

The spider has a number of options when configuring the ARC, but may only choose one. If a node's ARC is not known, or needs to be generated randomly, use the Random Alert Response table, p. 238, *SR4A*.

**Launch IC:** With this configuration, the node immediately runs one IC program. The particular program that is launched is chosen by the spider when the ARC is configured.

**Scramble Security Hacker:** When an alert is initiated with this configuration, the node will contact one designated spider or security hacker specialist (chosen in advance) and report the alert. It will also automatically log the spider or hacker onto the node, opening a subscription; this does not require a Log On action by the hacker.

**Terminate Connection:** The node immediately makes a single attempt to log the attacker out of the system (see Terminate Connection, p. 238, *SR4A*) when the alert is activated. When this test is made, the +4 bonus to Firewall against the icon bearing the access ID of the one that triggered the alert is included in the dice





### A BRIEF HISTORY OF CRYPTOGRAPHY

While cryptography has been studied since ancient times, the mathematical science of finding strong encryption techniques and ways to attack them really took off during World War II. In the following decades, a number of strong encryption algorithms were developed. Attacks on these methods were difficult, and most required far longer than a metahuman lifetime to perform. Encryption was a safe and reliable way to secure information.

Then, in 2065, a researcher at the Universität Stuttgart named Heinrich Andrews published an academic paper on a new method of attacking encryption. The paper described a technique that utilized the computational power of the latest generation of processors along with a breakthrough mathematical algorithm. It seemed that encryption techniques were no longer as secure as they once were.

Despite attempts by various corporate and government agencies to suppress it, Dr. Andrews's paper was circulated quickly around the Matrix shadow community. Shortly thereafter, a new generation of Decrypt programs hit the Matrix, all using the freshly dubbed "Heinrich Maneuver" to speed up cryptanalysis attacks.

Research into newer and stronger encryption continues, but there have as yet been no new developments. For now, at least, the days of reliable encryption are gone.

pool. Additionally, a spider (or any user with an admin account) may spend a Complex Action to have the node make an attempt to terminate a connection; this may be done without an alert, but also without the bonus.

**System Reset/Shutdown:** The node may be configured to either shut down and stay that way, or to reboot.

*DangerSensei is consulting on a high-security node. He has arranged for patrolling IC to Analyze visiting icons, but he knows that any real security problem would best be handled personally. He sets the ARC to Scramble Security Hacker, specifying himself as the one to be contacted and connected. He then logs off and goes about his business.*

*One day, while DangerSensei is enjoying an actual stroll through an actual park, a hacker successfully intrudes into the node, but one of the patrolling IC programs spots him. An active alert is triggered, and the node immediately logs him on. He spends a Free Action to flip into VR, and quickly deals with the intruder.*



## SPIDERS

A spider is a Matrix specialist that helps guard systems against intrusion. Their job description includes system administration, system monitoring, and managing agents and IC. The duties of the spider also overlap with those of physical security, and they handle security drones and facility devices such as cameras, locks, sensors, and even weapon emplacements. The spider coordinates responses to physical or electronic intrusion, usually in the capacity of communications officer or tactical commander.

An effective spider is built much the same way that a good shadowrunning Matrix specialist is constructed (see *The Matrix User,* p. 32). Spiders use the same skills and abilities to perform their duties as hackers and riggers use in theirs. The main difference is in program loadout.

While still seen as untrustworthy, those technomancers who put their mysterious talents to good use professionally and within the community are helping to improve their reputation. Most technomancers are at a disadvantage in the security field, since spiders that rely on technology have had more time to hone their talents, but more and more experienced security technomancers are appearing on corporate ladders. Evo and Horizon seem to believe that the untapped potential of technomancers is worth an investment, and have hired a number of them to act as spiders at some of their facilities around the world.

## SAMPLE SPIDERS

Below are some sample spiders that a shadowrunning team may encounter directly or indirectly during a run. Each entry includes a short description and a block of game statistics. These examples, along with the Spider contact (p. 12, *Contacts and Adventures*) can be used "as is," or modified to fit a particular node or setting. The statistics given are only those related to the Matrix; gamemasters should feel free to flesh out these examples with appropriate skills and gear. These examples give stats for humans; spiders of other metatypes should have their attributes adjusted accordingly (p. 4, *Contacts and Adventures*).

### Casual Hacker (Professional Rating 0)

Casual hackers have read some Matrix sites, done a bit of programming, maybe even jumped into a drone at one point. They are hobbyists or just the unlucky person at the office who was tagged for the job.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 3 | 2 | 2 | 3 | 3 | 3 | 2 | 2 | 6.0 |

**Skills:** Computer 2, Data Search 2, Software 1, Cracking Skill Group 1, Etiquette 3, Pilot Ground Craft 2, Current Events Knowledge 3
**Gear:** Contact lenses (w/ image link), AR gloves, sim module, trodes
**Commlink:** System 2, Response 2, Firewall 2, Signal 3
**Programs:** Analyze 2, Browse 1, Command 1, Edit 1, Encrypt 1
**Matrix Initiative:** 5
**Matrix IP:** 2
**Matrix Condition Monitor:** 9

### Novice (Professional Rating 1)

These spiders are usually either in or just out of college or an apprenticeship program, or are gifted self-starters. They occasionally make mistakes, either in their configuration or their responses, but they try their best to keep their systems secure.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 3 | 2 | 3 | 2 | 3 | 3 | 4 | 3 | 5.7 |

**Skills:** Computer 3, Data Search 3, Hardware 2, Software 2, Cracking 2, Etiquette 2, Perception 1, Pilot Ground Craft 3, Pilot Aircraft 1
**Gear:** Goggles (w/ image link, smartlink), AR gloves
**Cyberware:** datajack, sim module
**Commlink:** System 3, Response 3, Firewall 3, Signal 4
**Programs:** Analyze 3, Armor 3, Attack 3, Bio-Feedback Filter 2, Browse 3, Command 3, ECCM 2, Edit 3, Encrypt 3, Medic 2, Track 2
**Matrix Initiative:** 6
**Matrix IP:** 2
**Matrix Condition Monitor:** 10

### Security Technomancer (Professional Rating 2)

Technomancers are the newest entry on the security scene. Those that specialize in security face prejudice and distrust in addition to hackers and other digital attackers in the course of their duties.

| B | A | R | S | C | I | L | W | ESS | RES |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 3 | 3 | 2 | 4 | 4 | 3 | 4 | 6.0 | 3 |

**Skills:** Electronics Skill Group 3, Cracking Skill Group 3, Compiling 3, Decompiling 2, Registering 2, Etiquette 3, Perception 1, Pilot Ground Craft 3, Pilot Aircraft 2, Gunnery 2
**Living Persona:** System 3, Response 3, Firewall 3, Signal 2
**Complex Forms:** Analyze 3, Armor 1, Attack 3, Bio-Feedback Filter 3, Command 2, Track 3
**Matrix Initiative:** 9
**Matrix IP:** 3
**Condition Monitor:** 10

### Professional Spider (Professional Rating 3)

These spiders have been professionals for several years. Most of them like the job, and have settled into a confidence that ranges from informality to cockiness.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 3 | 2 | 3 | 2 | 3 | 4 | 4 | 3 | 5.0 |

**Skills:** Computer 4, Data Search 3, Hardware 3, Software 3, Cybercombat 4, Electronic Warfare 3, Hacking 2, Con 2, Etiquette 3, Perception 2, Pilot Aircraft 3, Pilot Ground Craft 3, Gunnery 3
**Cyberware:** Commlink, sim module, datajack, control rig
**Commlink:** System 4, Response 3, Firewall 4, Signal 4
**Programs:** Analyze 4, Armor 4, Attack 3, Blackout 3, Bio-Feedback Filter 4, Browse 3, Command 3, ECCM 3, Edit 2, Encrypt 4, Medic 3, Scan 3, Track 4
**Matrix Initiative:** 7
**Matrix IP:** 2
**Matrix Condition Monitor:** 10

#### Security Consultant (Professional Rating 4)

Security consultants are experts in their field. Some manage the defense of large or sensitive nodes. Others travel from facility to facility, bringing the security procedures up to speed during each visit.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 4.8 |

**Skills:** Electronics Skill Group 4, Cracking Skill Group 4, Con 3, Etiquette 3, Perception 4, Pilot Aircraft 3, Pilot Ground Craft 4, Gunnery 4
**Cyberware:** Commlink, sim module (w/ hot-sim), control rig, datajack
**Commlink:** System 5, Response 4, Firewall 5, Signal 4
**Programs:** Analyze 5, Armor 4, Attack 4, Blackout 4, Bio-Feedback Filter 5, Browse 3, Command 4, ECCM 4, Edit 2, Encrypt 4, Medic 3, Scan 4, Track 4
**Matrix Initiative:** 9
**Matrix IP:** 3
**Matrix Condition Monitor:** 11

#### Risk Management Engineer (Professional Rating 5)

"Risk management engineer" is a corporate euphemism for a digital operative: loyal to the corporation, dedicated to their jobs, and cold as the machines they use. They can protect a target electronically and physically, or completely erase it from the world and the Matrix.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 3 | 3 | 3 | 2 | 4 | 5 | 4 | 5 | 3.9 |

**Skills:** Electronics Skill Group 5, Cracking Skill Group 5, Con 4, Etiquette 3, Perception 4, Pilot Aircraft 4, Pilot Ground Craft 5, Gunnery 5
**Cyberware:** Commlink, sim module (w/ hot-sim), control rig, datajack, encephalon (Rating 1), math SPU
**Commlink:** System 5, Response 5, Firewall 5, Signal 4
**Programs:** Analyze 5, Armor 5, Attack 5, Black Hammer 4, Blackout 4, Bio-Feedback Filter 5, Browse 3, Command 4, ECCM 4, Edit 2, Encrypt 5, Exploit 5, Medic 3, Scan 5, Track 5
**Matrix Initiative:** 11
**Matrix IP:** 3
**Matrix Condition Monitor:** 12

#### Matrix Support Specialist (Professional Rating 6)

In the Unwired Age, electronic security keeps soldiers alive just as much as armor does. These military Matrix specialists cover military operations from the lowliest commando squad all the way up to the largest division. They are prepared to lay down their icons and their lives to complete their mission.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 4 | 4 | 4 | 3 | 4 | 5 | 5 | 5 | 2.65 |

**Skills:** Electronics Skill Group 5, Cybercombat 6, Electronic Warfare 6, Hacking 5, Con 4, Etiquette 3, Perception 4, Pilot Aircraft 5, Pilot Ground Craft 5, Gunnery 5
**Cyberware:** Commlink, sim module (w/ hot-sim), control rig, datajack, encephalon (Rating 1), math SPU, simsense booster
**Commlink:** System 6, Response 6, Firewall 6, Signal 5
**Programs:** Analyze 6, Armor 6, Attack 6, Black Hammer 5, Blackout 5, Bio-Feedback Filter 6, Browse 3, Command 5, ECCM 5, Edit 2, Encrypt 6, Exploit 6, Medic 5, Scan 6, Sniffer 5, Spoof 4, Stealth 5, Track 6
**Matrix Initiative:** 12
**Matrix IP:** 4
**Matrix Condition Monitor:** 11

## INTRUSION COUNTERMEASURES

Intrusion Countermeasures, or IC (pronounced: "ice") also helps protect systems from intrusion. Technically, an IC program is just an agent that is designated for security work, much the same way that "black IC" is just IC that carries one of the

### SCRIPTING

A script can take the form of an actual script, a list of conditions and actions that the IC runs through when acting. For example, a script for the MCT Bloodhound might look like this:

1. Is there an active alert?
   a. If yes, then go to 2.
   b. If no, then go to 5.
2. Has the intruder already been Tracked successfully?
   a. If yes, then stand down.
   b. If no, then go to 3.
3. Perform a Track on the intruder. Go to 4.
4. Does the Track finish successfully?
   a. If yes, notify spider of intruder's location and access ID. End action for this Initiative Pass.
   b. If no, end action for this Initiative Pass.
5. Perform Matrix Perception Test on the icon that has been Analyzed least recently. Go to 6.
6. Is the Analyzed icon an intruder?
   a. If yes, initiate an active alert and End action for this Initiative Pass.
   b. If no, end action for this Initiative Pass.

This format is longer and more involved than a brief description, but reflects the IC's limited decision-making abilities. When using this method of scripting, remember to make sure that every numbered entry can be reached from another (except the first, which is where the IC starts), and that every entry either leads to another entry or ends the IC's turn in the Initiative Pass.

programs designated as "black programs." No matter the name, most veteran hackers have stories about IC, with a mix of good and bad endings.

IC is versatile, but only a program. It has the same limited decision-making capability that agents do, and while IC programs are quite adept when handling situations for which they were designed, they tend to have difficulties dealing with novelty (see *Pilot Programs,* p. 245, *SR4A*). Gamemasters should keep this limitation in mind when determining the responses of IC programs during play.

A good way to "pre-handle" this limitation is by creating a *script* for the IC ahead of time. A script is simply a description of how an IC program acts or reacts. It usually takes the form of a few sentences of description, but can be more technical, depending on the preference of the gamemaster or player. The descriptions of the programs in Sample IC, below, contain scripts in descriptive form.

### IC Design

When designing IC, one should consider several factors. First, what it the purpose of the IC? Is it to stand alone against intruders? Will it be working with a spider or with other IC? Is it intended to patrol the node, or to only be run when a system alert is initiated?

Another factor to consider is the capacity of the node on which the IC is to be run. The IC program itself counts as one program for the purposes of reducing Response (see Response, p. 222, *SR4A*). Any programs the IC needs to run and use also count against this limit. An IC program running Attack, Armor, Analyze, Track, and Medic counts as six running programs, which will slow even the best commlinks and many medium-sized nodes.

Next, decide ahead of time how the IC will react to different situations. An IC program is an agent, and as such has a limited "common sense" that it can use to react to situations. IC can be confused, however, when faced with a situation outside the bounds of what it expects. To prevent this, most IC designers try to anticipate the situations in which the IC will need to act, and create appropriate scripting for it.

Another important but often overlooked aspect of IC design is iconography. Seen in virtual reality, the Matrix is a place where form need not follow function. What appearance does the IC have? What does its icon look, feel, sound, and even smell like in virtual reality? What actions does it perform when it runs its programs? Does a Terminate Connection action take the form of a bouncer throwing the hacker's icon out a window? Does IC with an Attack program take the form of a Knight Templar with a sword, an Amazon with a bow, or even a clown with a pie? Keep in mind that in most nodes, the icon that represents the IC will fit the theme of the node's sculpting.

## SAMPLE IC

The following are examples of off-the-shelf IC programs available from vendors both reputable and shady. Because they are designed for use out-of-the-box, they usually have very simple design or an easy-to-use set-up interface that presents itself to the owner the first time it is run. Each entry includes a description of the IC's standard behavior and the icon it uses when running; both of these can be modified by the owner. The rating of pre-packaged IC is also the rating of its loaded programs. Where a pre-packaged IC has one or more program options, the rating of those options is equal to half of the rating of the IC, rounded up.

Gamemasters are encouraged to design their own off-the-shelf IC programs. Keep in mind that such IC is designed to be simple, or to fill a niche. The cost of pre-packaged IC is equal to 0.9 times the sum of its component programs.

### Baby Swarm

This wicked piece of combat IC is a formidable opponent. It appears in VR as a large number of baby creatures, configurable to be anything from chicks to kittens to metahuman infants. When activated, it swarms through the entire node, attacking everything that it is not expressly configured to ignore. It is often kept running in a node, partially to cut down load times, but mostly because it is considered "cute."

**Loaded Programs:** Attack (with Area option, plus Armor Piercing option at IC Rating 4 or greater), Armor

### Encryption Prescription

Also called the "Encryption Conniption" by professional hackers, this simple IC program was written by students and licensed for sale by a number of small vendors. It appears in a node as a tubby cartoon doctor, complete with black bag and stethoscope. When it is activated, it immediately begins to use dynamic

encryption on the access log of the node and continues until it is stopped by an authorized user or it crashes.

**Loaded Programs:** Encrypt

### Ixcuiname

This devastating IC appears in virtual reality as a bulbous middle-aged woman that vomits a nauseating filth. When activated, it strikes its target with a psychotropic version of Blackout. Once it has successfully hit and inflicted its psychotropic payload, it attempts to terminate the target's connection.

**Loaded Programs:** Blackout (with Psychotropic option)

### Juhseung Saja

Courtesy of the Choson Seoulpa Ring, this ruthless black IC appears in virtual reality as a kindly older man or woman in traditional Korean garb. When activated, it initially attacks an intruder with Blackout. Once the hacker is rendered unconscious, the IC Tracks her signal back to the source and Spoofs the hacker's node to transfer the Juhseung Saja to itself. It then Browses through the hacker's node to find information about the hacker's family and friends, and then moves on to Track them, Spoof them, and attack them with Black Hammer. If it successfully kills the hacker's loved ones, it returns to the hacker and finishes her with Black Hammer.

**Loaded Programs:** Black Hammer, Blackout, Browse, Spoof, Track

### MCT Bloodhound

This IC patrols a node, using Analyze to look for intruders. Upon detecting one, this IC immediately starts Tracking, and reports the intruder's access ID and location to its owner as soon as that information is found. It is designed to be kept active in the node with both Analyze and Track loaded, for a total of three programs running. Its icon is a neon green hound with a black MCT logo emblazoned on each of its flanks.

**Loaded Programs:** Analyze, Track

### Renraku Oniwaban

This insidious IC is normally used with a honeypot (see *Tips and Tricks,* p. 72). It can be run in two modes: lethal and less lethal. It runs quietly on a node, concealing itself with Stealth. It attacks when an icon performs an action that is on a list configured by the owner (for example, when a certain file is edited, or a certain program is unloaded), or when a system alert is triggered. When it can be seen, its icon appears as a dark red or dark blue shadow.

**Loaded Programs:** Black Hammer, Blackout, Stealth

### Rumpelstiltskin

This offensive IC from Saeder-Krupp is designed to aggressively hunt down intruders and harass for their hacking attempt. Upon activation, the IC loads its programs and simply assaults the target construct with its Attack program until the intruder leaves. Its icon appears as a translucent version of the character from fairy tales that is its namesake.

**Loaded Programs:** Armor, Attack

### Singularity Encore

This program's icon looks like an idealized caricature of a media star manager. It is used in conjunction with other IC programs. It's job is to stand by in a node and immediately use the Run Program or Agent action on any program or IC that crashes.

**Loaded Programs:** none

### Three Musketeers Suite

This suite from NeoNET is actually three IC programs used in conjunction: Athos, Porthos, and Aramis. Each IC program has a different task. The Athos program runs a Track program on the user while the Aramis program runs Attack against the intruding icon and Porthos runs its own Attack program to crash the invader's programs (selected at random). This suite is expensive in terms of nuyen and processing power, but many hackers have found it too effective for their liking.

**Loaded Programs:** Attack x 2, Track, each with the Ergonomic option.

### Transys Florence

This IC program is used in support of other IC. Its task is to use its Medic program on any icon on its list, which is configured

| Pre-Packaged IC | Availability | Cost (up to Rating 3) | Cost (up t o Rating 6) |
|---|---|---|---|
| Baby Swarm | (Rating x 3)R | Rating x 3,825¥ | Rating x 8,100¥ |
| Encryption Prescription | (Rating x 3) | Rating x 945¥ | Rating x 2,340¥ |
| Ixcuiname | (Rating x 3)R | Rating x 3,375¥ | Rating x 5,175¥ |
| Juhseung Saja | (Rating x 3)R | Rating x 2,745¥ | Rating x 5,940¥ |
| MCT Bloodhound | (Rating x 3)R | Rating x 1,395¥ | Rating x 3,240¥ |
| Renraku Oniwaban | (Rating x 3)R | Rating x 2,250¥ | Rating x 4,950¥ |
| Rumpelstiltskin | (Rating x 3)R | Rating x 1,800¥ | Rating x 4,050¥ |
| Singularity Encore | (Rating x 3) | Rating x 900¥ | Rating x 2,250¥ |
| Three Musketeers Suite | (Rating x 3)R | Rating x 4,050¥ | Rating x 9,450¥ |
| Transys Florence | (Rating x 3)R | Rating x 1,350¥ | Rating x 3,150¥ |
| Watanabe Electric Kitsune | (Rating x3) | Rating x 945¥ | Rating x 2,340¥ |

by the owner. It can make its own decisions about prioritization, or it can be given a priority list. It appears in the Matrix as a white bird wearing a traditional nurse's hat.

**Loaded Programs:** Medic

#### Watanabe Electric Kitsune

This program takes the form of an anthropomorphic fox with configurable gender and outfits. Its task is to politely greet icons as they enter a node and help direct them to the appropriate resources. It also performs a Matrix Perception Test on every icon that enters, and continues to check icons while idle, starting with the least recently Analyzed. If it finds an icon that lies outside of the parameters with which it is configured, it triggers an active alert.

**Loaded Programs:** Analyze

## SYSTEM TOPOLOGY

Another way to secure a system is by putting it together in a way that is easier to secure. Much the same way that castles and secure facilities have physical configurations of walls and entry points that are more easily defended than others, Matrix systems can be built with security in mind.

## TIPS AND TRICKS

Security is not merely statistics and Matrix attributes. A system can be protected by a strong combination of policies, procedures, and topologies. The strategies and tactics offered below are just a small sampling of the expert spider's bag of tricks.

#### Backups and More Backups

One simple way to protect important files and programs is to make copies on a recurring basis and store them in an encrypted and/or protected archive. By comparing the current programs and files to the backups at regular intervals (from once a week for low-security systems up to every hour for high-security), a spider or agent can detect backdoors, viruses in programs, and altered files. The damaged files and programs can then be fixed by overwriting undesirable icons with the backups.

#### Chokepoints

The less a spider has to monitor, the easier it is for him to secure. Networks of nodes need more resources for security than a single node.

One way to limit the vulnerability of a large network is to allow only one or two nodes that act as gateways to the rest of the system. The rest of the nodes in the network are then kept behind wireless-impeding materials or are linked by fiber optic cables and have no wireless capability at all. Much like a checkpoint in a real-world facility, when all traffic enters at a single point, a spider can keep the network secure by monitoring only those nodes that have outside access.

This does not prevent an attack from within the system, usually executed by physically entering the facility that the network serves and accessing inner nodes directly. This falls under the spider's physical duties, along with those of the physical security of the facility.

#### Communication Protocols

A good spider remembers to secure the most vulnerable part of her system: the users. The strongest Firewall and IC in the world are no match for an idiot employee with clearance, and a good hacker knows it. A spider can put into place certain rules of communication to be followed by the users in a facility to help protect against a social engineering attack.

For example, a shadowrunner might make a commcall into a facility posing as a high-level executive in order to steal a passcode from a night clerk. If that clerk is aware of a policy in place that states that no management will ever call except on certain lines, or that they will use certain code words when making such calls, the chances that the clerk will divulge sensitive information is drastically reduced.

#### Cryptosense Sculpting

Though unusual, some systems use cryptosense simsense data in their system sculpting—sensory data such as ultrasound, thermographic, etc. A user who does not have a proper cryptosense module (p. 196) and who does not possess that physical sense will not be able to interpret the data. This will not prevent a hacker from making Matrix operations, but the lack or confusion of sensory details might inflict a –1 dice pool modifier to some actions (gamemaster's discretion). Use of a reality filter will override cryptosense data.

#### Decoys

Decoys are files and nodes that appear to be more dangerous than they actually are. By running a Stealth program that targets a file, a node can make that file appear to be larger or smaller,

filled with a high-rating Data Bomb, archived with strong IC, or anything else a spider can invent. The node can also use Stealth on itself, masking its true Matrix attributes, running programs, or other pieces of information normally garnered by a Matrix Perception Test.

When a node is using a decoy, the gamemaster should roll an Opposed Test, per the normal Matrix Perception Test rules involving Stealth (p. 228, *SR4A*). If the observer gains no net hits, she instead receives one piece of fictional information that the Stealth program is configured to give. This technique may only be used with files and nodes.

Decoys can be especially effective when used with a honeypot.

### Honeypot

A honeypot is a file or node that appears to be valuable to an attacker, but in fact is a trap set to lure intruders. All of the personnel that have genuine access to the system are aware of the honeypot's true nature, and are instructed to leave it alone. This means that any icon that attempts to access the honeypot is likely to be an intruder.

Honeypots are usually implemented in two ways, either as a decoy masquerading as an important file or node, or a ruse that appears to be a weak spot in the system's security. A decoy is usually only visible to security or admin accounts and encrypted, attached to a Data Bomb, or otherwise protected by security measures reserved for important files and nodes, to support the deception. As a ruse, they honeypot has low security and is used either as an indicator or a diversion into a non-critical node designated for such uses, often filled with IC or spiders. In either case, the honeypot is often placed where a hacker can find it.

Honeypots are often used in conjunction with patrolling IC that are scripted to watch for icons accessing the honeypot. A more advanced form of this strategy uses several honeypots that all appear identical to the actual important node or file, forcing an intruder to guess which is truly valuable and which is a trap.

### Layered Access

A spider can use an "onionskin" approach to security. In this method, the network is configured to have multiple gateways, each leading to the next. Unless the attacker can access the target node directly, she will be forced to work her way into a desired target one node at a time, slowing the attack and giving the system a chance to defend itself.

### Limiting Account Privileges

Employees at a secure physical facility are not allowed to be in areas to which they do not require access as part of their jobs. Likewise, users in a secure system should not have access to actions that are not critical to their performance. A simple way to do this is to deny lower account levels the ability to do certain things, such as see some or all of the files or subscriptions in the node, making or accepting commcalls, running certain programs, etc.

Likewise, accounts are often watched and/or restricted in terms of how many connections may be logged into them at a particular time. In this setup, the system assumes that if two or more entities are logged in under the same account, one of them is a hacker. This security feature is tempered by the fact that many users run autonomous agents, and these agents usually have access to their accounts. Nevertheless, some spiders configure their systems to automatically refuse any account login after the first, to closely scrutinize multiple logins, or at least limit simultaneous logins to a small amount in order to deter bots and malware.

### Passkey Checking

A system that uses a passkey system will initiate an alert when the access log shows the activities of a user that does not have a proper passkey, usually (System) Combat Turns after the start of the hacker's intrusion. For many governments, corporations, and other entities that have spent serious budget on a passkey system, this is not soon enough. Adding patrolling IC or spiders, specifically Analyzing icons for the proper passkey, is good for shortening intrusion times to a few seconds, if that. See *Passkeys,* p. 64.

### Protected Access Log

The access log does not offer much in the way of protection for a node, but it can help track down intruders after the fact. Disallowing the ability to see, read, or edit the access log to accounts below admin will help protect it against hackers. Another possibility is to Encrypt the log, if the node has the processing power to spare; this will only slow an attacker, however.

Yet another possible but unwieldy solution is to store the access log in another node. This requires a dedicated link and node access on the other node, but might confuse an intruder enough to keep the data that the system collects about him.

### Rebooting

Shutting down a device and allowing it to reboot will remove an intruder from a node with a Complex Action. In fact, it will remove all users from the system at the end of the Combat Turn in which the Reboot was initiated. The system then begins to start up again the following Combat Turn (see Reboot, p. 231, *SR4A*).

However, it is not always feasible to reboot a node, even for a few seconds. Marketing computers, security control nodes, medical mainframes, Matrix traffic hubs, corporate work servers, and military analysis devices are all machines that have critical applications that require the system remain up and running.

A system can be set to automatically reboot when an active alert is initiated, whether it be by the Firewall, IC, or a user with appropriate account access. This is not always desirable, and many systems leave the decision to reboot in the hands of a spider. High-priority nodes disable the rebooting option completely, and can only be rebooted by physically disconnecting the power from the hardware.

### Remote Spider

Having a spider on-site ensures that a system has a living person available and (usually) in the node, ready to handle security breaches. However, many spiders choose to work remotely. This allows them to confront intruders without the vulnerabilities that can be associated with an opponent in one's node of residence (for example, if an intruder successfully hacks into a node and gains

admin privileges, that hacker can simply deactivate and delete a spider's programs because they are running on a node on which the hacker has an admin account).

### Resident Programs

A node can run its own programs that operate automatically. All secure nodes that can afford it in currency and processing power should run Analyze, which automatically scans for hacking attempts (see *Matrix Perception and Topology,* p. 57). Encrypt is another program that should be considered for nodes, although the decryption of high-traffic nodes is often too cumbersome for users.

### Specialized IC

Intrusion countermeasures are invaluable against attackers, but IC with too many loaded programs can take too long to deploy against an agile opponent. Several IC programs with their own specialized duties, on the other hand, deploy faster. This is more expensive in terms of software and program count, but may be the deterrent that keeps hackers out of a system.

## SYSTEM DESIGN

The way a system is designed reflects a lot about the owners, the people it serves, and the system itself. Nodes are often sculpted for effect, whether to increase morale at the office, impress customers, or just for aesthetic impact. It reflects the values and beliefs of those who regularly use it, or at least of its administrators.

A Matrix system can say a lot about its users. A military installation is likely to have rigidly controlled topologies and utilitarian sculpting with unit insignias, while a commune might have a bizarre conglomeration of agglutinated nodes in a tangled mesh of a network.

### BUILDING A SYSTEM

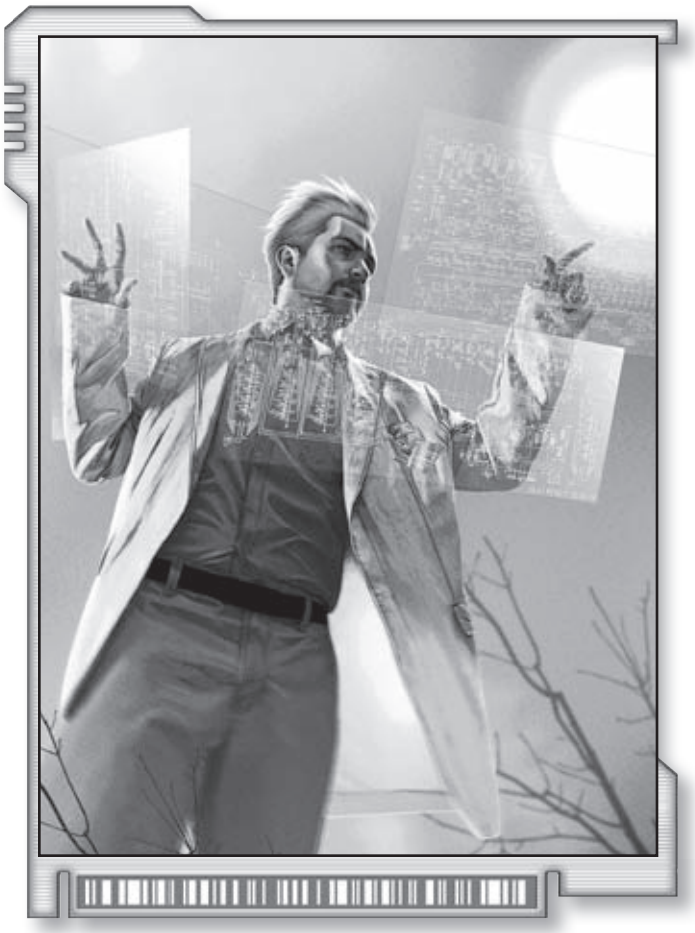
If you need a system for an adventure, and do not already have a fitting one from the examples below or another source, you will have to design your own.

### Purpose

Networks do not generally exist solely to have shadowrunners infiltrate them. Every Matrix system exists for a purpose. Some entity purchased the equipment, someone uses it, and someone maintains it.

The first thing to do when sitting down to create a Matrix system is to determine the system's purpose. Is it the main node that runs a secure shipping facility, or a book bindery? Will it serve many users or few? Do the users need subscriptions for the network to serve them? Are the users on the same site as the system, or are they telecommuting? What kind of budget does the system owner have? The answers to these sorts of questions will help you determine the size and shape of the network.

A properly designed system will be able to serve the personnel and devices that are to use the system. In general, a node should be able to handle at least one persona per user, and those personas should be capable of holding a subscription for each



peripheral device (such as sensors, locks, and gun emplacements), or at least for each group of devices. The program load for the system should be able to handle one or two programs per construct.

> *The gamemaster needs to design a Matrix system for an underwater kelp farming and research facility run by Aztechnology. She decides that it will be a large installation, with about 120 workers, a team of about a dozen scientists, and an engineering staff of 24. It is a large production facility with seven domes and a medium to large budget.*

### Topology

The shape of the network can contribute to its security, but more often it is dictated by its utility. If, for example, there are three independent labs in a building, each is usually given its own node. While the virtual environment of the Matrix is a place where the shape of an object has no bearing on what it is or does, the topology of a system is very much an example of form following function.

Start by establishing the nodes your system will need in order to perform its primary function, and determine the physical location of devices within the facility served by the network. Once that is in place, and if there seems to be an appropriate amount of budget left, add nodes for security, for example as chokepoints or gateways to the rest of the system.

You also need to choose the Matrix Attributes for the nodes in the system. For simplicity, you can assign identical Attributes to all nodes, or you can "personalize" each node's ratings. A system's average Matrix Attributes will be based on the level of importance of the system. See the Matrix Entity Ratings sidebar for ideas about what a node's average Attributes should be.

*The gamemaster decides that each dome will be capable of running independently, in case of a hull breach in one of the other domes, so each dome will have its own node. One of the nodes will double as the administrative node, one as the science and medical node, one as the engineering node, and one as the control node for all of the various drones used for farming. The others will be used by personnel for entertainment and other utilities.*

*All of the nodes will be connected via fiber optic cable, since the water around each dome will make wireless signals nearly useless. She adds a node that is connected via a fiber optic cable in the facility's surface tether to the rest of the Matrix, used as a chokepoint.*

*The facility is important, but it is not vital, so the gamemaster assigns Matrix Attributes of 3 or 4 to each node, as she deems appropriate.*

### Sculpting

The sculpting of a system is almost always determined by the one footing the bill. However, good management practices suggest that the sculpting be determined by those who most often use the node. This usually falls to a nodes administrator, or to a consensus of users.

When choosing the sculpting of a node, consider both the users of the node and the purpose for which it is designed. The users will want to work in a comfortable environment and be able to easily perform their duties.

*The facility belongs to Aztechnology, so the gamemaster decides that their logo will be prominent in all nodes. To help counteract the claustrophobia of dome life, the VR sculpting is an outdoor area, complete with weather and fresh air, where users are allowed to fly. Controls for various subsystems are contained in trees, rocks, and other natural features.*

### Security Allocation

As has been mentioned, most Matrix systems are intended for other endeavors than security. Most of its assets will be allocated to those purposes. Generally speaking, only ten to twenty-five percent of a system's resources (mostly its persona limits and processor load) will be dedicated to defense, including remote spiders and IC (which mostly take up processor load). Particularly secure or sensitive nodes will often increase this allocation to around fifty percent.

Note that this allocation is for passive security only. During active alerts, all of a node's available resources are often taken up in the defense as spiders deploy IC and programs.

#### MATRIX ENTITY RATINGS

The average Matrix attributes of a system are almost always a function of the owner's resources, professionalism, and influence. A high school club is not going to have the resources of an international bank. One way to choose the average Matrix Attributes of a system is to determine the professionalism of the entity sponsoring the node.

**Unprofessional (Rating 1-2):** These nodes tend to be cheap or cobbled-together bits of hardware and software. They are run by hobbyists, kids, small or medium-sized street gangs, and the like. These nodes are unimportant, which ironically gives them a psychological layer of security.

**Professional (Rating 3-4):** These nodes make up the bulk of the Matrix. Shops, small to medium businesses, contractors, organized crime, political parties, government offices, and other groups make up this level of professionalism. These groups may have something to protect, but nothing that is of life-threatening importance.

**Highly Professional (Rating 5-6):** This level is reserved for megacorps, major governments, militaries, and individuals and organizations that are very rich, very powerful, or both. They are serious about their Matrix systems, and an intrusion at one of them can cost millions of nuyen. Particularly sensitive sites can have Matrix attribute ratings greater than 6.

*The gamemaster determines that the system can afford to have each node have its own IC patrolling, and another IC program loaded but not running.*

### Spiders

Any facility that employs security will most likely have at least one spider. Some will only have one or more spiders, relying on the spiders' drones and devices in the real-world environment rather than hired muscle to cover physical security. For the most part, a facility will employ one spider for every thirty to fifty other personnel, or about one per squad of physical security, or one per two or three nodes. The Professional Rating of the spiders is usually very close to the highest System rating of the nodes in the network.

*The gamemaster decides that three spiders would be about right for they system, given the number of personnel and nodes. She uses the sample spiders from this chapter, making the Head of Matrix Security a Security Consultant, and the other two Professional Spiders. For style, she decides that the three spiders use a "ship's bells" style of taking duty shifts.*

Urgent Message...

### QUICK AND DIRTY SYSTEM DESIGN

All gamemasters have had creative players. The team's technomancer has an idea, and suddenly you need a system for the local public access simsense channel. Here are two ways to keep the action moving and provide a system quickly.

**A Rose by Any Other Name**

One quick and dirty way to generate a system is to use one of the sample systems from this book, and file off the serial numbers. An FBI office system in Seattle probably looks a lot like a BIS Büro network. Just take the same system, but rename the node, change the description and sculpting, and you have a new node. If you want to differentiate further, add, subtract, or exchange one or two of the spiders or IC listed for another from the samples given in this chapter.

**The Magic Number**

If you cannot find a sample system that could serve for the node you need, use this more abstract approach. Choose a "magic number" to act as a rating for the entire network, and simply use that rating for everything within that system. This includes the Matrix Attributes of the node or nodes, the ratings of IC and programs, and the Skill and Attribute ratings of spiders. Choose an ARC that you like, or use the Random Alert Response table, p. 238, *SR4A*.

#### IC

Remember that a lot of IC is restricted, and so requires either licensing or permission from some authority. A non-profit entity is unlikely to have IC that uses restricted programs. On the other hand, most corporations and governments lack that constraint. Black IC is a particularly violent way to keep intruders out of a system; it should only be used for systems that have or would have physical defenses that use dangerous or lethal force.

*Aztechnology is a megacorp, and wants to protect its investment, so the gamemaster pulls no punches when assigning IC to nodes. She chooses relatively innocuous models for the patrolling IC, but makes the loaded IC chock full of nasty, especially in the administrative and chokepoint nodes.*

#### Resident Programs

There are only three programs that a node might be running independently. The first is the Analyze program, which helps watch for hacking attempts. The second is Encrypt, which should only be used for encrypted nodes. The third is Stealth, if using the decoy technique for security.

*The gamemaster decides that the seven internal nodes are too heavily trafficked for encryption or decoying, but every single one runs Analyze, just in case.*

#### ARC

Finally, choose an alert response configuration for each node in your network. You can assign the same configuration to every node, or individualize them. Keep in mind that when one node in a network initiates an alert, all nodes go on alert.

*The gamemaster chooses the Launch IC ARC for all of the nodes in the network. A would-be intruder will be in for a nasty surprise.*

## SAMPLE SYSTEMS

Every system in the Matrix is different. Some are sculpted. Some are heavily traveled. Many are similar, being born of off-the-shelf devices that have been personalized by the owner. Some are made of a single node, some are made of several. All of them have security against digital intrusion.

The following are descriptions of some systems from around the world in the 2070s. These systems can be used by gamemasters as the basis to design systems encountered by players in their games.

#### The Ork with the Gold Tooth Bar, Seattle, UCAS

This seedy little hangout is one of the very few places in Redmond to offer any kind connection to the Matrix. Naturally, it is a proving ground for hackers trying to escape the barrens and shadowrunners alike.

**Sculpting:** The node is dim and grungy. It attempts to look like a classier tavern, but its environment software has needed an upgrade for several years. There is a glitchy routine animating fake-looking artificial patrons singing raucous drinking songs that skip randomly. The IC uses an off-the-shelf icon of a male Ork with the owner's face badly bitmapped to its head.

**Hardware:** The node is actually run on an old Sony Emperor that has been welded to a pipe under the bar. There are also two cameras and a satellite uplink, all slaved to the main node.

**Authentication:** Passcode
**Privileges:** Standard
**Attributes:**
Node 1: Firewall 2, Response 2, Signal 3, System 2.
**Spiders:** 1 Casual Hacker (the bar's owner)
**IC:** 1 at Rating 2, no programs. IC runs at admin privileges. Terminates the connection of intruders.
**ARC:** Terminate Connection
**Topology:** The single node is the master for one external camera, one internal camera, and one satellite uplink, all of which are slaved.

#### Brent Cross Shopping Centre, London, UK

This state-of-the-art mall serves the shopping needs of some eight million consumers. Among its many features, its node offers directory services, virtual fitting, VR day care, digital concierge, and automated valet parking.

**Sculpting:** The node looks a lot like it does in real life, but with more flash. Most of the architecture is translucent, and patrons who buy a membership are allowed to fly and to pass through walls.

**Hardware:** Fifteen custom Renraku Retailer Hubs (Persona Limit 10, Processor Limit 20)

**Authentication:** Web of Trust (SIN verification)

**Privileges:** Standard, plus registered users receive targeted coupons.

**Attributes:**

Nodes 1–15: Firewall 4, Response 3, Signal 5, System 3.

**Spiders:** 3 Professional Spiders on duty at all times.

**IC:** 1 Watanabe Electric Kitsune 3 per node (patrolling)

**Resident Programs:**

Nodes 1–15: Analyze 3

**ARC:** Scramble Security Hacker

**Topology:** Fifteen identical nodes, each linked via wireless in a mesh.

### Undergraduate Matrix Lab, Cambridge, UCAS

This tiny hacker's den is tucked into a corner of the MIT&T campus. It is popular system for young hackers and is often the site of pranks, both on and by the system administrators. It is an excellent example of a clever security design without top-of-the-line hardware.

**Sculpting:** The sculpting in this node changes from semester to semester. It often includes popular culture references, beavers, cutting-edge animation, and even some sports iconography if the Engineers are doing well this season.

**Authentication:** Varies, usually Linked Passcode, occasionally Other Authentication Method

**Hardware:** Each node changes from term to term, and each is unique (Persona Limit 10–25, Processor Limit 20–50)

**Privileges:** Standard, but a large percentage of registered users have security and admin accounts.

**Attributes:**

Nodes 1–4: Firewall 5, Response 2, Signal 2, System 4

**Spiders:** A random mix of Casual Hackers, Novices, and Professional Hackers, with the occasional Security Technomancer. There are 1–6 spiders in the system at any given time.

**IC:** 1 MCT Bloodhound 4 per node (patrolling), other IC (loaded) which varies according to students' whims

**Resident Programs:**

Nodes 1–4: Analyze 4, occasionally Encrypt 3

**ARC:** Variable; use the Random Alert Response table, p. 238, *SR4A*

**Topology:** Nodes 1 through 4 are linked via wireless in a mesh. Each uses decoys to prevent access from one to another.

### Dante's Inferno, Hong Kong

Like the famous and incrementally exclusive club in real life, this system has multiple layers of access. Each node is a painstakingly sculpted version of the real Dante's Inferno in the Central District, complete with virtual glass dance floors to give patrons a look at the icons dancing in the nodes "above" and "below."

**Sculpting:** The virtual decor in each node is modeled after each of ten Buddhist hells. Each node appears as one of the dance floors in the real-world version of the club, except that the size of the virtual room changes based on the number of patrons within it. Special guests are given "super powers," such as the ability to fly or dance on the walls and ceiling.

**Hardware:** Sony Spectacle Nexus (Persona Limit 10, Processor Limit 35)

**Authentication:**

Nodes 1–9: Passcode

Nodes 10–11: Passkey

**Privileges:** Standard, plus user access allows a construct to appear in the real-world AR system.

**Attributes:**

Node 1–3: Firewall 3, Response 3, Signal 3, System 3

Node 4–6: Firewall 4, Response 3, Signal 3, System 3

Node 7–9: Firewall 5, Response 4, Signal 3, System 4

Node 10–11: Firewall 5, Response 4, Signal 2, System 5

**Spiders:** 1 Security Consultant and 1 Professional Spider on duty at all times.

**IC:** 2 Watanabe Electric Kitsune 3 w/ custom sculpting per node (patrolling)

**Resident Programs:**

Node 1–6: Analyze 3

Node 7–9: Analyze 4

Node 10–11: Analyze 5, Encrypt 5

**ARC:** Scramble Security Hacker

**Topology:** Node 1 is open to the Matrix and available for wireless access. Each of Nodes 1 through 10 are connected sequen-

tially via cable, with wireless access available to each node from each corresponding level of the club. Each of Nodes 1 through 9 act as a gateway to the next node in sequence. Node 11 is connected to each of the nodes via fiber optic cable. Nodes 1–10 also have holographic systems and cameras slaved.

### BIS Büro, Hamburg, Germany

The *Bundesamt für Innere Sicherheit* (Bureau of Internal Security) does not have much sway in the Free City of Hamburg. They do have enough of a presence to warrant an office in Wandsbek. Their system is typical of many non-secret government offices.

**Sculpting:** The sculpting is clean and utilitarian, with marble and wood finishes. The BIS emblem is prominently displayed.

**Hardware:** One MCT Sentinel II (Persona Limit 10, Processor Limit 60) and one NeoNET Office Genie (Persona Limit 5, Processor Limit 20)

**Authentication:** Passkey

**Privileges:** Standard

**Attributes:**

Node 1: Firewall 5, Response 4, Signal 4, System 5

Node 2: Firewall 5 Response 3, Signal 2, System 4

**Spiders:** 1 Security Consultant on duty at all times

**IC:**

Node 1: 1 MCT Bloodhound 5 (patrolling), 1 Three Musketeers Suite 5 (loaded)

Node 2: None

**Resident Programs:**

Node 1: Analyze 5

Node 2: Analyze 4

**ARC:** Launch IC (Three Musketeers Suite)

**Topology:** Node 1 is accessible from the Matrix via wireless, and acts as a gateway for Node 2. Node 1 is the production node, Node 2 is an archival node where the office's records are kept.

### Choson Lair, Various Locations

This is actually one of many similar systems used by the Choson for their operations. Each Lair is run on hardware that is easily packed up and transported, so they can create a Lair, use it for as long as necessary, and then shut it down and store it or move it to a new location as needed.

**Sculpting:** The sculpting for each Lair is different, based on the purpose of the node and the preferences of the administrators, but all have a red-and-yellow yin-yang design worked into the design.

**Hardware:** Custom Choson portable nexus (Persona Limit 5, Processor Limit 45)

**Authentication:** Passcode

**Privileges:** Standard

**Attributes:** Firewall 4, Response 3, Signal 5, System 4

**Spiders:** 1 Professional Spider on duty at all times.

**IC:** Juhseung Saja 4 (loaded), Watanabe Electric Kitsune 4 (patrolling)

**Resident Programs:** Analyze 4, Encrypt 4

**ARC:** Launch IC (Juhseung Saja)

**Topology:** Single encrypted node.

### Tux's, Seattle, UCAS

There's no hotter spot on the 'Trix than Tux's, the VR night club for the preeminent hacker. Tux's requires that its patrons hack their way in, and moves its physical location almost every day (sometimes hiring shadowrunners to insure the secrecy of the move).

**Sculpting:** The sculpting in Tux's is completely random, and subject to the whims of its patrons. Normally a consensus is reached at some point each night, but the occasional "sculpting battle" rages through the VR landscape.

**Hardware:** [need info from Topology chapter] Changes access ID every night.

**Authentication:** No access allowed.

**Privileges:** All privileges moved to admin.

**Attributes:** Firewall 5, Response 4, Signal 6, System 5

**Spiders:** none, except for the patrons, usually Security Consultants and Risk management engineers

**IC:** 1 Rumpelstiltskin 4 (patrolling)

**Resident Programs:** Analyze 5

**ARC:** Terminate Connection

**Topology:** Single node connected to the Matrix via wireless.

### Diez de Octubre Airbase, Aztlan

This installation is an open secret in the heart of Durango. Many wild rumors of magical jet fighters and unnatural research abound about this military base, including one that states that this is the site of an ultraviolet node.

**Sculpting:** The sculpting is a sterile white environment. The flag of Aztlan is here, along with a number of military insignias.

**Hardware:** Custom system (Persona Limit 20, Processor Limit 65). Access ID changes every night.

**Authentication:**

Node 1–3: Passkey

Node 4: Alchemical Passkey

**Privileges:** Standard

**Attributes:**

Node 1–3: Firewall 6, Response 5, Signal 4, System 5

Node 4: Firewall 6, Response 7, Signal 2, System 7

**Spiders:** 1 Matrix Support Specialist and 1 Risk Management Engineer on duty at all times

**IC:** 3 Renraku Oniwaban in each node (patrolling)

**Resident Programs:** Analyze 6, Encrypt 6 on all nodes

**ARC:** Scramble Security Hacker (Matrix Support Specialist)

**Topology:** Node 1 serves as the air control node. Node 2 handles physical security and drone command. Node 3 is the administrative node for the base. Node 4 can only be accessed on site within a Faraday cage, and has no connections to other nodes.

### Zurich Orbital Terrestrial Substation, New York

This network handles unimaginable amounts of transactions worth an indescribable amount of money. Many a hacker has been left brain dead trying to make a run on this system.

**Sculpting:** An impressive stone hall greets users logging on to the system. Archways lead to different nodes, each carefully secured for privacy and against intrusion.

**Hardware:** Saeder-Krupp Schwermetall high-security nexus (Persona Limit 25, Processor Limit 110)

**Authentication:**

User: Linked Passcode

Security and Admin: Nanotech Passkey

**Privileges:** Standard, plus user accounts may make transactions on their own accounts

**Attributes:** Firewall 9, Response 8, Signal 4, System 8 (all nodes)

**Spiders:** 2 Matrix Support Specialists and 4 Risk Management Engineers on duty at all times

**IC:** 3 Watanabe Electric Kitsune 7, 2 Renraku Oniwaban 8, 2 Rumpelstiltskin 8, 2 MCT Bloodhound 8 (patroling)

**Resident Programs:** Analyze 8

**ARC:** Scramble Security Hacker

**Topology:** The topology is that of the onionskin, with a spiral of sixteen successive nodes. Each node is a gateway to the next. Node 1 has access via wireless to the Matrix. Each node is connected to the previous and following nodes by fiber optic cable. Nodes 2–8 are for standard clients, nodes 9–12 are for more exclusive clients, and node 13–14 are for exclusive clients. Node 15 handles both the administration and physical security in the building, and node 16 is connected to the satellite uplink.

### ABSTRACT MATRIX RUNS

Sometimes it is impractical to run an entire system during play. This is especially true when the entire group of players is present, and there is only one Matrix specialist at the table. In these cases, simply abstract the entire system into a single meta-node. Use the highest values of each attribute for the meta-node, along with as much of the IC and running programs as is feasible.

For example, the BIS Büro sample system would be abstracted to a single node with Firewall 5, Response 4, Signal 4, System 5, one Security Consultant, a patrolling MCT Bloodhound, and a loaded Three Musketeers Suite.

## SECURITY IN ACTION

So what does all of this look like in action? How might the various components of a secure system work to prevent, or at least slow, an intrusion? This is an extended example of the security involved in a hacking attempt. The example uses the Professional Spider from Sample Spiders, p. 68, and the Choson Lair sample node, above.

### SECURITY EXAMPLE

Jin, a Professional Spider for the Choson, has been assigned to secure a new Lair in Seattle. She is monitoring the node in AR, but her attention is focused on her morning soaps.

The node is running Analyze, Encrypt, and a Kitsune IC program. Additionally, the IC is running its own Analyze program, for a total of four programs, well below the sixteen-program limit of the node.

A hacker has broken the Lair's encryption, probed the system, and enters the node. The node is running Analyze, and makes a single Analyze + Firewall Test to detect the intrusion. The gamemaster rolls eight dice for the node and gets four hits, missing the hacker's Stealth by one hit. The hacker enters the node with a hacked admin account.

The Kitsune IC running on the node is programmed to check out new icons, and it does so. The Kitsune icon greets the intruder and performs a Matrix Perception Test using its own Analyze program, rolling eight dice in an Opposed Test against the hacker's Stealth + Hacking, which is a dice pool of 12. The IC rolls four hits, and the hacker rolls four; with zero net hits, the Kitsune finds nothing suspicious about this new icon, and allows the hacker to operate within the node.

The hacker performs a Deactivate Agent action to shut down the Kitsune program before it has a chance to see through his Stealth program. Since this action is allowed to users with admin accounts, there is no roll needed, and the Kitsune program's status switches from running to loaded.

Since Jin is watching the node, she makes a Matrix Perception Test to see if she notices the program being shut down, and succeeds. She performs a Log On action to activate a subscription and arrive in the node, using a Free Action to flip into VR. The hacker then performs his own action to accomplish his mission in the node.



Jin is suspicious enough to initiate an active alert, and does so as a Free Action on her next turn. The node executes its ARC, immediately launching the Juhseung Saja IC program. Jin then spends a Complex Action to load an Attack program, ending her turn.

The hacker sees the IC activating and recognizes its icon. He tries to get the system to unload it, figuring (correctly) that he might have more Initiative Passes than the spider and so buy some time. He rolls his Hacking + Exploit (a dice pool of 12) against the node's Firewall + System (8 dice). The hacker rolls five hits, but so does the node, so his attempt fails.

The IC loads its Blackout program, while Jin takes a shot at the intruder. She makes a Cybercombat + Attack Test against the hacker's Firewall + Response. She gets three hits, while the hacker only gets two, and causes 4 DV of Matrix damage. The hacker manages to resist all of this damage with his System + Armor, but only barely.

At this point, the hacker decides to bail, and disconnects from the node. Jin shuts down the Juhseung Saja IC and assesses the damage. The node's file system has been compromised, and the hacker got away with the data he wanted. However, he did not have time to remove his datatrail from the node's access log, and Jin runs and then uses a Track program using that information. She finds out that the hacker was making his run from the Pine Cone Restaurant near I-90, and sends that information to operatives in the field. She goes back to her soaps, knowing that even if the operatives investigate the restaurant, the hacker will be long gone.

# . . . HACKER'S HANDBOOK . . .

Pistons's reality filter slipped and fizzled as she passed through the gateway, her perfect color-coded polygons giving way to a romantic programmer's dream of a Japanese garden, her icon now wearing a black ninja gi. Fourteenth century stone bridges contrasted badly with the twenty-first century koi emulations swimming in the brooks beneath them. Sloppy work, or else they were more interested in security than historical accuracy.

Whipping out a rice-paper fan, Pistons frowned as she analyzed the icons in the node. Intrusion countermeasures, but they haven't detected her yet—and that fox with seven tails was the gatekeeper for the security controls she needed. Reaching into the satchel at her side, the hacker launched Tumblers. The agent appeared next to her as a man in a dark suit.

Whispering instructions under her breath, Pistons sent Tumblers toward the fox construct. A little stiffly, his iconography not quite matching the surrounding node, the agent presented one of the passcodes she'd hacked for this run to the fox. The vulpine gatekeeper's tails twitched in time as it processed the code before letting Tumblers pass.

Once the agent was seated at the ornate tea table, Tumblers started to run through his script, moving the controls in a precise pattern. Pistons noted that the fox program was still watching the agent, but she didn't care about that now—she needed to find out who else was lurking nearby.

Right on cue, a polychromatic Eastern dragon slithered into view, its mimetic scales and fractal coloring a pale imitation of the real thing. A sudden wind rustled through the garden, and the gentle ping from her Analyze program told Pistons the system had moved to Active Alert.

Tumblers didn't even fight the IC construct that latched onto his back, paralyzing the agent so the draconic security hacker could give the lazy kill-shot with an Attack program. Pistons bid a silent adieu to the agent, its job well done. As the dragon passed by her again and the fox resumed its previous stance, Pistons waited patiently for the wind to die down and the Active Alert to pass.

Cloaked by her Stealth program, Pistons took a knife—her Exploit program—and slipped it through the rice paper wall of the teahouse, bypassing the fox construct. A few minutes later, she slipped back out the same way, Tumblers' work—and hers—now complete. She took a few minutes to patch up the rent in the rice paper—it was still there, but hidden from prying eyes.

*After all,* she mused, *you never know when you might be here again.*

» Hacking lore keeps to the fringes of the Matrix. Upstanding citizens have no use for it, the powers that be want to keep it bottled up for their own ends, and the hackers themselves have little interest or benefit from sharing it. There are large portions of hacker history unwritten and unread, great hacks that would be legendary if the world only knew of them. As it is, would-be hackers have to read through the better part of a century's worth of lies, out-dated strategies, and self-styled hacker's handbooks to try to piece together the skills they need.

Screw that noise. This is the real deal, the true dope, a dose of the hacker's tools and the hacker's tactics for the here and now, from three of our resident experts.

» FastJack

## THE GRAY AND THE BLACK

**Posted By:** Glitch

From the beginning, hacking has dealt with doing things other people hadn't thought of yet (or at least not legislated against), skirting the edge of the legal by exploiting loopholes and language, and of course doing whatever you can because you can and no one can stop you, whether it's illegal or not. The line between the gray and the black can be a fine one, even in this day and age when Matrix crime is analyzed and defined in a hundred ways by thousands of lawmakers.

» If you want a good comparison, think of it as the difference between a gray market and a black market. On the grey market, things are a little shady and maybe you don't know where it came from, and every now and again the cops bust somebody with something. The black market is full of the scary guys from the megacorps and the syndicates and the military—but that's where the money, the freedom, and the power are.

» Mr. Bonds

The gray market of hacking is full of things that don't appear that harmful. Selling corp scrip in an area outside of corporate jurisdiction, writing a script to exploit a flaw in a game and sharing it with your buddies at school, using your mom's commlink for a few minutes to visit that node she doesn't want you to go to, using a flaw in the vending machine interface to get it to dispense a free Gooey Bar, sharing music on a peer-to-peer network. Lots of people make use of tricks like these to make their lives just a little bit easier, and some of them even lose sleep over it.

» Some of those things you've described are technically illegal, but if no one gets hurt, where's the harm, right?

» Turbo Bunny

» There's always the potential for harm. Maybe not to you, or your family, or your friends, but some corp or artist somewhere might lose a few nuyen, some poor bitch will be fired for having an obvious passcode, and some poor bastard will lose a night's sleep fixing gamecode when your exploit becomes widespread. It behooves us to think of the consequences of even the smallest rebellion.

» Kia

On the other side is the blatantly and grossly illegal that's bread and butter to most of us here, which is what most people think of when they say hacking. Damn near any criminal or terrorist activity you can think of has its Matrix equivalent: breaking and entering (hacking a node), extortion, protection rackets, and hostage taking (denial of service attacks, security consulting, and ransomware), arson and destruction of property (crashing a node, deleting files), release of toxic, radioactive, or biological weapons on a civilian populace (viruses, worms, and trojans), graffiti (AR graffiti), pornography, theft, etc. Hacking can also facilitate other sorts of crime, especially white-collar crime like stock fraud.

» These new takes on traditional crime are what the syndicate hackers are most involved in, and they can be very protective against newcomers encroaching on their "turf"—never mind how ridiculous that term might be with regards to the Matrix.

» Mihoshi Oni

### THE CRACKER UNDERGROUND

The freedom-loving specialists (or sometimes just aficionados) who break copy protection to see how programs work are called crackers. As socially aware beings dedicated to increasing the sum of metahumanity's knowledge by sharing the tools and information needed to obtain that knowledge, crackers congregate to share their liberated data. A cracker's street cred is made by cracking files and signing them with the anonymous handles they use to protect themselves from the data-dictators in the corporate world. Crackers cost the megacorps millions of nuyen every year trading in cracked software, taking back what should rightfully be free.

To protect themselves from corporate reprisal, crackers use security measures familiar to most hackers, including made-up names that define their digital persona (something everyone here should be familiar with, I reckon) and trade over anonymous peer-to-peer networks. The megacorps can and do infiltrate these networks, uploading viruses and bogus files to confuse and discomfit users before they're discovered and booted out, but these underground resources are what people turn to when they need cracked proggies.

In a perfect world, all software would be free. However, this is the shadow economy. Somebody went to a bit of risk and effort to liberate, crack, and post those illegal programs you need, and they expect a modicum of compensation. Of course, it helps that all the really, really good peer-to-peer filesharing networks are sponsored, maintained, and protected by the syndicates, and they want their cut too.

» Long story short: filesharing networks can be either flea markets or swap meets. You're either paying bottom dollar for your goodies, or you can grab all you want as long as you share the wealth. But oh what prizes you may run across! Just remember to disinfect everything before you run it.

» Slamm-0!

More sophisticated warez crews, particularly the ones run by Matrix gangs and the syndicates, have fancier operations. They use legal cover operations like casinos and online stores to maintain a stable web presence and launder their nuyen, and some of them have insiders in place who can get their hands on programs and media before they're released to the general public. These groups are completely mercenary in their philosophy, cracking and pirating solely for nuyen, often charging little less than the market price—or, for unreleased and military-grade programs, much more than their market price.

Urgent Message...

Don't call me a script kid
Don't call me a cipherpunk
Don't call me a cracker
Don't call me a data pirate
Don't call me a gray coder
Don't call me a Matrix criminal
Don't call me an information terrorist
I am a hacker.
~ Slamm-0!
01/27/71
Seattle Metroplex Grid

» Not that anyone in their right mind would want a prototype program—but hey, it's your brain. Let me know how it works.
» Pistons

» Hey, don't knock it. A buggy killer program from some corporate R&D obtained by your friendly Cyber Nostra is as close as some of us get to really bleeding-edge software.
» 2XL

## VIRTUAL PRIVATE NETWORKS

JackPoint is a virtual private network (VPN), so all of you should be aware of the basic interface: a single AR window or virtual screen with a limited text- and image-based interface instead of a real-time streaming simsense feed. Aside from hosting clandestine collections of criminals like us, VPNs are the backbone of Seattle's mobile social software (MoSoSo) tribes, the Cracker Underground's vast web of illicit file-sharing networks, MagickNet (for those Awakened aspiring to join the Sixth World and trade formulae), and bunches of eternally popular instant messaging services, among other things.

A virtual private network is only as special as the people that are on it, and the creators and maintainers of VPNs and their associated software usually take care to keep the riff-raff out when selecting members. It's very much like being a member of an exclusive club, and as is the case with exclusive clubs, privacy tends to be a big concern. Hence the reason JackPoint has a secure log-on and encryption, among other little tricks you probably haven't noticed.

» Please respect the network and try not to trace your fellow JackPointers or hack their passcodes. If you would refer back to the agreement you all made when you accepted the invitation, such actions invite repercussions from all of us—including me.
» FastJack

» Of course, there's nothing to keep you from going power-mad, becoming an overcontrolling asshole, and protecting your friends on the hugs-and-kisses squad.
» Clockwork

» Correct. Which is why you're free to leave at any time. Until I do enter super-villain mode, I'll be enforcing the rules strictly. Until your next infraction, you and your persecution complex can take a rest.
» FastJack

» I didn't break your damn rules.
» Clockwork

» That's the only reason you're still alive, mouth breather.
» Netcat

VPNs work by directly using connecting commlinks, employing mostly unused connection protocols that date back to the first incarnations of the Matrix. These protocols are mainly invisible or forgotten, buried under layers and layers of code. While limited in the content that can be transmitted and received, VPN 'ware can directly bypass Matrix Service Providers and commcodes, providing reasonably secure communication with a minimum of processing power or exchange of incriminating data.

» A VPN is only as secure as the encryption on the code, the secrecy of the members, and the paranoid moments of the people running it. The less you talk about JackPoint, the less people know about JackPoint, the more secure JackPoint is.
» Pistons

## PAYDATA

Information is a commodity in the Sixth World, and that's a fact that hackers and shadowrunners know better than most. There are plenty of runs where the primary objective is to get data at all costs, and plenty more where a little judicious browsing in a system paid off big-time when the datafiles were sold to the local fixer or data broker.

Urgent Message...

### THE EXCHANGE

One virtual private network of particular interest to shadowrunners, especially in and around the Seattle Metroplex area, is the Exchange. This program monitors your actions through your commlink and correlates that data with other users, tracking your needs and abilities with the geographic area you are in. At seemingly random intervals the program will prompt a user to take some non-threatening action with the promise of being "karmically rewarded" Common instructions include:

- Take a left and buy the guy on the corner a soykaf with extra sugar
- Leave a clip of ammo on the stairwell of the tenement down the block as you pass it
- Visit Rhiannon and talk to her about *Le Grand Grimoire* for at least ten minutes

While odd, each of these services helps out someone else in the network—by providing a distraction, or a critical piece of equipment, or just a much-needed cup of soykaf during a stake-out. All of the users on the Exchange that heed the prompts find themselves subject to strokes of luck and happy accidents in a similar vein.

Unlike most VPNs, the users have no other way to contact each other through the network, and no one knows exactly who is running it.

» You have to be careful about selling hot data. To get the best price you should delete the originals, but that means that you alert the owners of the datastore that they've been hacked. Not very professional.
» Cosmo

Data brokers are a distinct breed of fixers that specialize in buying and selling information. Some are backed by syndicates, others by corps or governments, but most are independent and prefer it that way. They deal mostly with incarcerated criminals, paparazzi, hackers, spies, and industrial saboteurs—but also with stock brokers, fixers, police, government officials, and even members of the intelligence community. Most data brokers have some background or interest that informs their preferences; a talismonger-turned-data broker (often called a loremonger) is probably more interested (and will therefore pay more) for thaumaturgical research, magical formulae, and metamagical theses than for the schematics to Ares's latest assault rifle.

Buying data is only half of a data broker's job; the other half is selling it. To that end, a data broker can be a very valuable, if mercenary, contact, able to get you nearly any sort of data for the right price.

» And because of the many areas of interest they walk in, data brokers tend to have some truly arcane connections. If they don't know what you want to know, they know someone who does.
» Fianchetto

» Ask a fence to find a fence.
» Kay St. Irregular

The one thing that can make a data broker antsy is if the data bears the marks of belonging to somebody with a fierce reputation. More than one hacker has been left holding the datachip when no data broker in town would touch a bunch of hot intel straight from the oyabun's nodes because of what the Yakuza will do to them if they found out about it. This kind of healthy fear/superstition is strongest in towns with one ruling syndicate or corp rather than megasprawls; in Seattle you can take your pick of the Yakuza's enemies and sell it to them. Hell, you can try to sell it a bunch of times—just don't get caught.

### Proprietary File Formats

Most megacorps (and some government agencies) put files that are strictly for internal use within the company, such as source code for programs and internal memorandums, in proprietary file formats (PFFs). Files encoded in PFF are normally only readable on the company's own operating system, though various hackers and crackers have made conversion utilities that allow the files to be accessed on any commlink, node, or terminal, no matter what OS is running. Data brokers like PFFs, as they offer a relatively simple measure of security and veracity to a datafile.

» You can make your own PFF datafiles. The necessary modules are generally included in all OS software, but they are only activated when a valid SIN belonging to a corporate employee is registered as the owner of the device. So if you steal a wageslave's commlink or log into their work terminal with a stolen passcode, you can save everything as PFF.
» Kat o'Nine Tales

» Or you could just hack your own commlink to activate the modules.
» Slamm-0!

» That would work too.
» Kat o'Nine Tales

### Certified Data

One of the lesser-known fallouts of the Crash 2.0 was the Corporate Court's release of an early version of the technology used to create certified credsticks as a way for major corporate and national banks and institutions to safeguard their data. The so-called "certified data" tech has slowly trickled its way down to the streets, and it now sees limited use in most sprawls for sensitive information that can't be trusted to the Matrix, like proxy votes for megacorporate shareholders or the passcode for some encrypted nodes.

Anybody with a chipburner and access to the Matrix can use the freeware utility provided by the CC to burn files as certified data. The certification process deletes any other copies of the files to be burned from the user's commlink and creates a special access log on the chip itself that logs all attempts to access the chip and its contents. Theoretically, the access log and the encryption scheme mean that any attempt to read, copy, or edit the contents of the chip will be logged (and might scramble all the data on the chip). There's nothing to prevent you from sending the files to a dead-drop node or even burn them to another chip *before* you certify the data, which is why the format was ultimately abandoned by the CC in favor of something with a look-back feature.

» Data brokers love certified data because it "proves" they're being honest with their clients. A good hacker can crack the protection on a certified datachip and make it look virgin when you've already squirreled away six copies in your anonymous dropbox.
» Cosmo

## THE FORGER'S ART

System Identification Numbers, permits, licenses, nuyen—it's all numbers my friend. No more than a pattern of ones and zeroes on a computer. There are many fixers and hackers that specialize in forgery, weaving lives together out of lines of code and sending it off to the proper databases. The shadow economy lives on fake SINs, and many shadowrunners burn through them regularly.

» No shit. It doesn't pay to skimp on your fake SINs. I did it once and ended up with some dead corper's SIN, straight from a shady morgue attendant who agreed not to register it for a few days. Three days later I've got half of Lone Star after me thinking I'm a damn shedim-infested zombie.
» Sticks

## SPOOFING LIFE

Hacking isn't just a career, it's a lifestyle—or it can be. By keeping a library of access IDs and spoofing the right commands, a hacker can effectively improve her lifestyle. To get it to work, the hacker has to keep her virtual eyes open all the time, keeping track of access IDs for power, water, Matrix access, rental agreements, grocery delivery—all the essentials of life—and issuing the

right commands to bring those things to her doorstep. Sooner or later the people the hacker is ripping off are going to find out and cut power, send her bills, reclaim property (and possibly break her hands), so a hacker spoofing her way through life has to be constantly juggling her needs and extras, re-issuing commands, switching services, and grabbing new access IDs all the time.

» The phrase "living on borrowed time" comes to mind.
» Icarus

## TOOLS OF THE TRADE

**Posted By:** Slamm-0!

Being a hacker isn't all about buying a better commlink or upgrading your warez—you want to hone your skills to compete with the likes of yours truly, and you'll need to learn a few of the tools of the trade that they don't teach in the after-hour comp-sci classes at the local pub.

### EXPLOITS

Any good hacker knows that an exploit doesn't just happen; you have to make it happen. If you wait for the perfect flaw to cross your path, you're never going to get anywhere as a hacker. You have to go out and look at the code, see where the ambiguity lies, and keep an open and creative mind for how to tweak your programs to take maximum advantage of the opportunities that exist.

When you get down to it, exploits are the most basic building block in a hacker's arsenal. Every attack program, every strategy or tactic for bypassing security, every hardware or software hack is based around an exploit of one form or another. Without an exploit, no user would have privileges beyond those basic access rights assigned to them. Without exploits, there would be no hackers.

» And the armies of darkness would march across the face of the Matrix ...
» Glitch

Most exploits aren't due to programmer faults or deliberate flaws placed in the program by skilled and foresighted hackers; they come about from translation errors or slight incompatibilities between different code, creating ambiguities that a skilled user can take advantage of to do things they aren't suppose to be able to do—such as bypass system security or other safeguards. The Matrix has so many layers of code that it is practically impossible to prevent exploits in code, not that programmers ever stop trying to make flawless code, or spiders stop patching up new exploits as they're discovered.

A new exploit is worth its weight in gold radicals, and hackers tend to hoard them—the less often an exploit is used, the less likely it is to be discovered and patched. On the other hand, data brokers (and even other hackers) are always on the lookout for a good exploit and will trade in cred or favors for them.

### BLACK MATRIX SERVICE PROVIDERS

People like us need to access the Matrix, and for that you need a Matrix Service Provider (MSP). Of course, without a SIN (or not wanting to give out a SIN), we need an MSP that will accept straight cred and not ask any questions: a black MSP. Some of these services border on the legal, providing the same services as regular MSPs without asking for SINs, while others are hacked accounts on a normal MSP or strictly illegal operations set up by Matrix syndicates, which tend to offer special services like anonymizers, one-shot commcodes, dead-drop e-mail boxes, and credit laundering services.

#### Anarkh

One of the many free shadowy MSPs available to shadowrunners and the SINless, Anarkh is a no-frills black MSP that offers only the most basic service—a commcode. But there's no ads and no charge. I wouldn't leave any files in your mailbox (ever), and it can be hacked by a couple college students on brainbenders ... but hey! Free!

#### Anonymizers and Re-Mailers

While not always illegal, a good portion of the anonymizers and re-mailers available on the Matrix are run by Matrix gangs, or as under-the-table start-ups by enterprising spiders and programmers in little-used corporate nodes. The advantage of the shadowy anonymizers is they don't have to work with law enforcement; the downside is that they're less trustworthy than legitimate Matrix security corps. Both cost about the same for their level of service.

#### Fuchi Telecomm

A lingering remnant of Fuchi Industrial Electronics, this splinter corporation was lost in the shuffle as the megacorps squabbled over the remains of the former AAA megacorp. Because of lingering contractual obligations, NeoNET has to allow Fuchi Telecomm access to the new Matrix protocols for existing customers. Of course, by the same obligations, Fuchi Telecomm can't accept any new customers, so there's a brisk under-the-table trade in existing accounts. Billing doesn't care to know the SIN as long as they're paid at the beginning of every month. They don't give you agents, but they do offer anonymizer and re-mailer services for a nominal fee.

#### One-Shots

A service exclusive to the larger and more organized black MSPs are one-shot commcodes, good for a set period of time (usually 24 hours after activation, though this varies from provider to provider) or the duration of a single continuous Matrix session (up to the maximum period), and then all traces of the commcode are erased. Shadowrunners usually use one-shots when they need limited Matrix access, or they don't want to worry about being sloppy.

#### Pusan Undernet

An affiliate of the Choson Ring in Seattle, the Pusan Undernet is typical of the larger and more organized black MSPs, the type that charges as much (or often more) than a comparable premium MSP but offers additional services in the form of one-shot commcodes, numbered credit accounts, and escrow services.

### BACKDOORS

In hacker parlance, a backdoor is a hidden account or deliberately programmed security flaw that lets you access a particular system easier. People can get really paranoid about backdoors because

they're ignorant and don't know anything about programming, so they always suspect the programmers that write the software for a particular node leave themselves a little way to get in whenever they feel like it. People that know something about programming, on the other hand, recognize this as grade A bullshit; the little wageslave coding his life away is never even going to *see* the node running his software, and if he was ever caught doing something as stupid as putting a backdoor in, he'd be fired, dragged downstairs to some lightless basement and shot, his pale and bloated corpse put up in the hallway by the watercooler to show the rest of the luckless corp programmers what fate awaits them if they try and get cute.

» When did the megacorps become Pol Pot?
» Baka Dabora

» Okay, so maybe not that bad, but more than one programmer has arranged for a self-extraction after a horrible fuck-up was discovered.
» Slamm-O!

No, the people who make hidden accounts are end-users, administrators that are trying to sneak in and out of the office node for a little cybernookie without it showing up on the access log, and maintenance monkeys that need to illicitly give themselves a higher level of access to fix everything that's gone wrong with a node because the stupid slitches in charge have degrees in Intercorporate Business Affairs and other poppycock instead of Matrix Systems Management. It's the shady security hacker looking to moonlight and the black ops division that needs an untraceable way in and out of their own corp's computers. And, of course, there are pure hackers.

» Every so often, you stumble onto a hidden account while watching somebody's traffic, or when you browse an access log and don't see a login when you know there was activity in the node.
» Kay St. Irregular

» Some nodes—especially Matrix brothels—have all of their customers register a hidden account and log in that way for anonymity. Nice way to ditch a tail if you've got the nuyen.
» Orbital DK

There's a division among hackers on the use of backdoors. Some prefer to use them sparingly, only placing hidden accounts in a few nodes where they might need emergency access, the argument being that there's less chance for people to catch you using a hidden account. Others like to use backdoors for nodes that we hack on a regular basis, letting our icons slip in and out whenever we need to, 'cause it makes our lives easier and we're less likely to get caught than if we were hacking the same node over and over again. No backdoor lasts forever, and at some point word of it gets out or an admin or spider will scan it and delete it. I tell ya, nothing's more embarrassing than trying to access a hidden account that's been deleted.

» Of course, sometimes the canny bastards just flag the hidden account and bushwhack you or start an automatic trace when you enter the node.
» Puck

## MALWARE

Matrix gangs and code punks use malware for the same reason they bust up cars or steal shit—to cause a little trouble, mayhem, and destruction. Granted, a virus doesn't get the blood pumping as well as an old-fashioned beat down, but there's a little adrenalin surge when your code goes out to trash some bastard's commlink real good.

Professionals, on the other hand, are much more selective. Both the Crash of '29 and the Crash 2.0 were caused by malware, and hackers today have more respect for both the destructive capability of a virus and its reputation. Those syndicates and Matrix gangs that are into computer crime make extensive use of malware as part of extortion schemes and protection rackets.

» Not to mention insurance fraud and disposing of evidence. Last year the Wanibuchi-gumi in Neo-Tokyo were laundering hundreds of thousands of nuyen through a little online bail bondsman—but they didn't remember to pay their taxes. When the taxmen started swarming the place, they launched hidden viral packets that destroyed the node, corrupting the evidence beyond repair—and letting the bail bondsman collect the insurance.
» Mihoshi Oni

A **virus** is a self-propagating piece of software that "infects" software of a specific type. Done right, this can be a simple and insidious way to cripple a network or automated factory. Serious combat hackers sometimes like to soften up nodes by feeding them viruses first; despite the propaganda you hear from the corps, only the most careless hackers end up infected by their own viruses during a run. Personally, I like to install a ticker virus tied to cyberware

drivers on my commlink before I turn it off for the night; most people don't think to disinfect immediately when they boot up, and anybody trying to jack my shit lets the virus spread through their PAN to their implants.

**Worms** are specialized malware agents with an emphasis on stealth instead of brute force. As long as you keep the agent from running the entire payload at once, a good worm can last for days or weeks on a node without being discovered. Corporate hackers and law enforcement tend to favor worms, especially dataworms, to keep track of hackers or limit their capabilities. One really nasty combination is to load a worm with a pacifist virus that infects the hacker's combat proggies and prevents them from frying the worm outright. On the other hand, worms themselves have few defenses against viruses. I usually stick with an inertia-infected autosoft to jam their replicate ability.

• Kinda sucks for riggers though, huh?
• Sticks

• The best defense for a drone is simply not to get hacked to begin with, but a good back-up for riggers is strong encryption—stymies most worms. In a pinch, a rigger that can't deal with a worm or a virus immediately is best off cutting it out of their network before the infection spreads.
• Rigger X

• Or shut the infected drone down and leave it as an effective booby-trap for somebody. I got burned like that once.
• Turbo Bunny

Private Message...

**From:** Clockwork
**Subject:** Re: Ergonomic Malware

Whether or not to load your malware with ergonomic programs depends on the purpose of the malware agent. If you want to slow down or crash the system, loading the malware with regular programs is a good way to go. On the other hand, if you want your malware to be undetected, I'd go with the ergonomic program option: less program load means it's less likely to be noticed. Sometimes you might even want to combine the two ideas. For example, maybe you want a worm to spread throughout a system (using ergonomic stealth programs to stay undetected), and then when the signal is given (or timer clocks down, whatever), the agent de-activates its ergonomic program and runs its regular programs to slow the system down. The only catch is that there's a period of time between activating and de-activating programs where the worm is particularly vulnerable.

Viruses and worms are both straight forward and proactive programs designed to weaken a node or device in some way. By contrast, **trojans** are more like scouts that go in and pave the way for a later hack.

• Of course, there's nothing to stop you from combining different types of malware. You can have a worm with a virus and a trojan in its payload that moves in, smoothes your entry, and unleashes the virus to cover your tracks when you leave. It's almost like creating genetic chimerae in its elegance.
• The Smiling Bandit

## AGENTS

Agents are essential to the function of the modern Matrix, and many hackers have at least one to help them with background tasks they don't have time to do themselves. An agent is really a presence multiplier for hackers, letting them expand the number of places that they can be in and what they can do. No surprise, then, that some hackers go for agents in a big way.

• Some hackers frown on the use of agents, especially when some brainless ape that knows jack-all about hacking uses a mook instead of figuring out how to do things themselves.
• The Smiling Bandit

• Mook?
• Sticks

• A high-end agent that does everything in the Matrix for the user, even the most basic tasks. Instead of learning how to hack, the user commands the mook to do it for him. Most MSPs provide basic agents to make the user's life easier, and lazy users just order them to do everything. Commercial mooks have built-in limitations against breaking the law. To build a mook capable of hacking, you need a real hacker.
• The Smiling Bandit

Another advantage agents can provide is that they are eminently disposable—if the agent gets crashed, the hacker can just re-load it. Still, hackers should be wary about feeding their agents to IC and spiders: unless you load it onto the node (which requires privileges most hackers don't have), the agent can be traced directly back to you. If you *do* load an agent on a node, you'd better be sure it doesn't have any incriminating data on it, because if it's found and dissected it can lead straight back to you—or the spider can research exploits to use specifically against that type of agent or the programs it carries, giving them an advantage over you in cybercombat.

The major limitations on agents are the number of active subscriptions they take up and the number of programs they can have running before seeing lag. Having two agents running at the same time can slow your commlink down something fierce. You can get around the lag by not running any programs yourself—only really an option if you're letting your commlink run overnight while you're not connected to it or something—or you can load the agent onto another node and let their system lag. When you upload an agent to run on another node, though, you still have to keep an active subscription to it to receive data and give it orders in real time. When you want to use more agents than your commlink could handle on its own, the next step up is a botnet.

• Note the key word there is "in real time." Hackers that don't mind the snail's pace and uncertainty of knowing whether or not their agent is still active and running can sever the active subscription and let the agent just run on its own until the hacker re-establishes contact, or a hacker and agent can forward their communications through an e-mail account or use other non-real-time communication methods.
• Glitch

## BOTNETS

Normally when you load an agent onto a different node from your commlink, you maintain an active subscription to that agent, issuing orders and receiving feedback in real time with a minimum of hassle. Naturally, your active subscriptions limit the number of agents you can have running at once. To get around that, instead of maintaining active subscriptions you can link your agents into a network—a botnet. A botnet isn't as slick as an active subscription, but if you're looking to recruit a codezombie army of doom, it's a good start.

By itself you might think a botnet is simply a useful tool for managing a lot of agents, but the implications for hackers are huge. With a botnet you can keep tabs on dozens of nodes at once, setting up some truly righteous hacks. Most really organized Matrix gangs and syndicate Matrix crime crews use botnets for distributed denial of service (DDOS) attacks, extending their traditional protection rackets and blackmail operations into the Sixth World. A DDOS attack uses scores or hundreds of bots on different nodes to connect to a single node at the same time, usually preventing all traffic into and out of the node—quite a killer for a commercial node, and well worth it to online merchants to pay a "protection" fee against the possibility of it happening to them.

• Sometimes when you can't pull off a big hack, you can use a botnet to pull off a lot of little hacks that add up to the same thing. Perfect example: traffic control. Hacking the individual lights and using bots to control them can be a hell of a lot easier than hacking the central traffic node.
• Turbo Bunny

• Unless, like in Hong Kong, all of the traffic lights are slaved to the central node anyway, in which case you have no choice but to hack it. Or in New York, where the lights are tied into the GridGuide system for better traffic flow control.
• Traveler Jones

See, it's not just hackers that use botnets—it's corps too! How do you think AZT manages its fleets of spambots, or MCT datafarms millions of customer datafiles every day? Their experts use botnets to direct and control fleets of agents, and if you know what to look for you can take control of one or more of their bots and get them to work for you—at least, until the wageslave managing the botnet notices something weird is going on.

While the corps don't like to talk about it, botnets are also a way for them to wage war on one another through the Matrix. It's a rarely used tactic for a megacorp to directly fuck with another megacorporate node with a botnet because of the fear of reprisals from the Corporate Court; current Matrix warfare theory holds that if two AAA-rated megacorps decided to engage in a full-scale Matrix conflict, botnets would feature prominently in the strategy.

# THE ART OF WAR

**Posted By:** Pistons

To a combat hacker like me, the Matrix is a battlefield. Espionage, siegecraft, stratagems, the parry and thrust of cybercombat. The kid's covered some of the basic weapons you'll have in your conflicts across the Matrix, so what you need now is the down-and-dirty of the tactics hackers use. A little strategy and the right weapon can win any war.

## MASS PROBES

The key to a successful botnet isn't getting a lot of agents—you can copy those programs for free. What you really need is a large number of nodes to run your agents on. That's where a mass probe comes in. It starts off by having a large list of potential targets—hacker nexi usually have dozens of these lists around, but you can use the Yellow Pages node if you really want to. There are different strategies and mathematical formulae to optimize the methodology, but in essence a mass probe is a very quick and direct attack on a node to see if it responds—if it does, you break off quick, if it doesn't you log it. Either way, you move on down to the next node on the list. After a couple hours of dedicated probing, you'll have a list of poorly defended nodes that should be a cinch to load your agents into.

• You can also mass probe to create a botnet and then have the agents on the botnet mass probe and replicate to create more botnets, etc. That's how the most malicious worms spread. The Grid Overwatch Division and local authorities keep an eye out for that type of thing, though, and try to nip it in the bud.
• Cosmo

## MASS ATTACKS

Hackers are generally solo types, untrusting and untrustworthy of other hackers.

• Hey! I resemble that.
• Puck

Still, hackers also have a long tradition of teamwork and cooperation with other hackers for really big hacks. A mass attack is just

what it sounds like: two or more hackers combining their skills and resources to infiltrate a given node. It has to be a slow hack unless you want to just bust in, but it's pretty effective. The problem with mass attacks is that once you're inside the node, alliances tend to fall apart quickly—different hackers want different things, and they sometimes end up fighting each other and node security at the same time. Hey, you know what they say about trusting criminals ...

## PHISHING

While hacking your way into a system is one way to gain access, it's often loud and noisy—the Matrix equivalent of breaking the glass and reaching through the hole to unlock the door while hoping you haven't set off any alarms. A quieter, stealthier way is to look under the mat for a key first—or in Matrix parlance, get a passcode and access a legitimate account. Getting passcodes or other personal data off of a mark is called phishing.

When you go phishing you need a lure or bait—something to entice the mark or open up a line of dialogue with them. Common phishing lures include an online store or e-mailed offer. A false online store (also called a *phishing trap*) often acts just like a real one, displaying goods and then taking customer information—including their identities, contact numbers, and shipping addresses—so that you can deliver the product. Phishing lures can also include viruses and other malware that infect customers as they come in, a good way to snag passcodes. Trojans are particularly easy to use if you can disguise them as a "free trial offer" of a new AR software or something like that.

• If you don't mind the cost, the site can even be functional–I know one hacker that started out making an online organic jams distributor and made so much honest cred from passing traffic that she got out of hacking altogether. Of course, she had to apply for business licenses and the like.
• Mr. Bonds

E-mail phishing attempts (*line casting*) are often caught by spam filters or discarded out of hand because they don't interest the mark. Personally, I like to combine the phishing lure and line casting by setting up a fake site geared toward the mark's interests and then sending a coupon or introductory offer to them. Naturally, this requires some knowledge of the mark and their interests.

• A phishing lure can also be used to set up a botnet; you just load a hidden bot on every "customer" that enters the node to browse or shop.
• Glitch

Once you have their personal and financial data (which pretty much means their SIN number and authorization on their online bank accounts), you can clean them out—which is where a lot of phishers get caught. It's one thing to duplicate a charge for a meal and make it look like the restaurant deducted the cost twice, but it's something else again to blow somebody's life savings on a piece of gear and then have it mailed to you. Keep in mind that any online purchases you make can be tracked back to you. Smart phishers will siphon off some cred to a certified credstick and then disappear with it.

More sophisticated phishers target megacorps and financial institutions, often using a lot of social engineering to masquerade as someone who would legitimately have access to the (usually very well protected) personal or financial data. Theoretically you could set up a bank or other financial institution as a big phishing lure, but I've never heard of anyone that managed it.

• It's difficult to pull off because banks, credit unions, and non-bank financial service institutions have a lot of regulations, even in the most unregulated parts of the world (I'm looking at you, Carib League). Still, more than a few venerable financial institutions began as phishing lures until the owners and operators realized they could milk ten or a hundred times more nuyen out of a steady clientele than they could ever take from a single megacorp. And then there's the handful of orgs that were bought out by the Mafia and the Yakuza.
• Mr. Bonds

## DENIAL OF SERVICE

Denial of Service (DOS) attacks are proof that ancient hacker philosophy never goes out of style (though it may fall behind the tech curve). DOS attacks are about locking a user out of their commlink or terminal, or more often preventing a node or commlink from accessing the rest of the Matrix by flooding it with incoming connections. The how and the why might change each time, but the basic goal is the same—denying someone Matrix service.

The key to most DOS attacks is overloading the target with traffic, with botnets being the weapon of choice. A hacker with a big enough botnet can inundate the target with data requests, connection requests, and other forged signals, locking out other incoming traffic. Spiders and IC can try to filter out the bot traffic or spoof their node's access ID, but sheer numbers usually swing things in the botnet's favor.

A DOS attack on a commlink is a little more difficult, because you first have to perform a successful trace on the target icon; you can also lock someone out of their commlink or node with a little judicious editing of the connection filters, cutting them off from practically the entire Matrix. If you have the time and skill to mess with the accounts, you could even change all of the passcodes to keep the legitimate information technology personnel from fixing the problem right away.

Anything else that prevents people from accessing the target works too—crashing the operating system on a node, physical damage to a key server or optical trunk that supports traffic in and out of the node, switching the node to hidden mode—anything your dirty, clever little minds can think of.

• I had a job a couple months back where my group was hired to do a 24-hour DOS attack against the node of a corp that was going to release a new product online that day, but our hacker gal got sick and couldn't perform. Ended up having to cut the optical trunk and aim a HERF rifle at it all day. Then the punks tried to switch to a satlink, and I ended up blowing that up with a missile! So much for a nice, quiet Matrix job.
• Beaker

## RANSOMWARE

By itself, a DOS attack is normally a means to an end, not an end in and of itself. Script kiddies may get their jollies locking some poor bastard out of his home terminal so he can't turn in his homework or show up in his virtual classroom, but more often than not a DOS attack is part of the growing Matrix-based extortion phenomena. The idea behind Matrix extortion is simple: individuals, corporations, even governments need access to the Matrix and certain files.

Without that access, they can't buy food or make money, along with a thousand other essential things in life. If you threaten or take control of a node or certain files—through a DOS attack or some sort of malware, or anything, people will pay for the safe return of their goods. This sort of criminal activity is usually labeled ransomware.

One specific and popular type of ransomware involves a hacker penetrating a node's defenses and then encrypting key files, usually tied to a data bomb or some malware that will activate if someone tries to decrypt the files without the correct passcode. Encryption ransomware works best on individuals, particularly if the data files are of a sensitive nature, because decryption programs are restricted to corporate hackers and licensed freelance security consultants.

• In the spirit of the street finding its own uses for things, there are a lot of tools and tricks that corps use to secure their own nodes that can be turned around to prevent them from accessing them. My favorite security trick is to install a passkey requirement on a node and then reboot it, dumping all the current users. When they go back to log on, they don't have the passkey and get blocked.
• Slamm-O!

The corporations are well aware of ransomware and its repercussions, so don't be surprised if you're on the receiving end of it some time. I knew a Mr. Johnson for NeoNET that paid us up front but encrypted the certified credstick and slapped some IC on it as a form of security; we knew the Johnson would pay because we could see the cred, but we couldn't spend it until we finished the run and he gave us the passcode to disarm the IC and decrypt the cred. Sneaky bastard.

• A lot of data brokers turn around and sell the datafiles they buy back to their original owners for a significant mark up. The nasty ones sell the corp encrypted datafiles then charge them more for the passcode to decrypt them.
• Cosmo

## HACKER TRICKS

More than riggers, hackers focus on the virtual space of the Matrix rather than the nitty-gritty infrastructure that supports it. That's not to say a hacker won't take optical trunks and mesh networks into account, but they're less likely to be scanning the airwaves or worry about it as long as they have a solid connection to the 'trix.

### Hacking Cyberware

Sometimes, it's easy to forget that all that chrome doesn't mean jack shit without the software running it. That is, until you get an interface problem and two pieces of 'ware don't want to talk to each other—then it comes to the forefront of your mind. Nowadays, it's easier to hack cyberware than ever before, and shadowrunners should pay close attention to how their implants are wired together.

Most cyberware is set up as peripheral nodes connected to your PAN during implantation, and configured for open access so that medtechs can access the implants quickly for diagnostics and repair. Most internal implants are usually accessible with a low-level wireless connection.

• Shadow clinics and street docs with a little programming expertise can disable this wireless connection if the client asks, arrange for the

implant to send out false diagnostics, or even upgrade the software without much trouble.
• Butch

• Okay, but does that mean that if I get into a fight with a hacker or technomancer they can just reach out and turn off my cyberarm?
• Hard Exit

• Maybe, but probably not. Cyberarms and most implants that have an exposed area on the body often require direct wired connections through access ports and the like, not a wireless signal. If you're really worried about it, you should keep your cyberarm in hidden mode—or better yet, turn it off. Not always the best option, but it prevents hacking.
• Butch

Like any other device, implants are susceptible to viruses and other malware. The devices most at risk to this sort of tampering are those connected together through direct neural input (DNI)—in other words, any implant that you can control with a thought. To prevent a single virus or worm from infecting all of their systems, many street samurai and other implant-heavy runners front-load a high firewall on critical access points like datajacks. If the malware can't get past the datajack, it can't infect the rest of the DNI implants in your system.

• Cyberware hacking can work to your advantage too, though. Just as an example, most people don't realize that a smartlink is wireless. That means you can send a command to your smartgun even if you're not holding it. And a hacker can spoof a command to that smartgun as well.
• DangerSensei

• Yep. You can also stick malware into a smartgun (which'll spread to infect your smartlink) or crash it to prevent it from firing.
• Slamm-0!

• In modern warfare, it is common practice to use malware and databombs to disable equipment we must leave behind—or worse, erase the equipments' operating system.
• Picador

### Subscribed Commlinks

Nowadays, just about anybody without a PAN is obviously a criminal hacker or a technomancer. Walking down a busy street in Hong Kong in hidden mode is the equivalent of trying to look inconspicuous with a day-glo mohawk. To avoid looking like a putz, you can keep two commlinks: a public, legal POS and your real commlink loaded with all of your tasty illegal programs. Just subscribe the public commlink to your hidden one, and you can walk around like a normal person.

• Keeping a legit commlink has other benefits than just to hide your hidden commlink, especially for SINners. You can keep all of your above-board accounts and e-mail separate from your shadow life.
• Kat o'Nine Tales

• Some hackers go overboard with subscribed commlinks, daisy-chaining them together into a "stack" for various purposes, like being in more nodes at once or having more agents under their direct command available. These amateurs like to think they can "hop" from one commlink to another and avoid the damaging effects of IC—hey, if I'm not there, it can't hurt me right? Wrong. Unless you logout of the node, your icon is still present—whether you're paying attention to it or not, and damage from Black IC still hurts you directly.
• Slamm-0!

• Why can't you just have the commlinks running separately?
• Sticks

• Because no matter how many commlinks you have, you only have one brain. All of the data is going in there, and if you try to use two commlinks at once you'll get a splitting headache, multisensory hallucinations, and your icons will try to do the same thing on both commlinks at once. The way around that is to link the commlinks together—daisy chaining, as I said—so that you're only focusing on one icon at a time (even if each icon is in a bunch of different nodes), flipping through the stack.
• Slamm-0!

### Social Engineering

It's an old axiom that the weakest link in any security system is the metahuman element, and that holds true for the Matrix as well. Good old fashioned social engineering is updating the ancient confidence trick to the digital realm of the Sixth World, preying on the better or worse natures of your fellow metahumans to gain access to a node or device. It's amazing the variety of old scams that can be adapted to the Matrix, or the new ones that have emerged over time.

At its heart, social engineering has nothing to do with your hacking skills or your programs; it has to do with your ability to understand and manipulate other people—which can be tricky, as in many cases you need never meet the other person face to face. Often, social engineering can involve elaborate "sets" (nodes/AR ads dressed up to look like they belong to a legitimate company or government office) or the use of publicly available information to convince the mark of the validity of the company or that you are a legal employee of it. In many cases, the goal is information (e.g., a passcode, an account number, client personal details, a SIN, a list of nodes), and the social engineer tries to convince a user with legitimate access to that information to share it on some fabricated pretext, such as an accident, insurance claim, or research.

The benefit of social engineering is that you don't have to risk your fanny hacking a node to get basic data that a secretary or customer service rep has immediate access to; the downside is there's no guarantee it'll work. It should come as no surprise that corps spend a good bit of time drilling proper information safeguards into their employees' heads to combat social engineering, so don't be surprised if the first secretary you meet seems skeptical bordering on paranoid.

• Social engineering could be as easy as masquerading as a worker at a Matrix brothel and seducing a security weenie to gain intel on a node, or as elaborate as hiring sim actors to play their respective roles and put the mark in the middle of a drama. My favorite cons involve marks that are betrayed by their own lust or greed.
• Dr. Spin

• How very Shakespearean of you, Doctor.
• Pistons

They key to social engineering is fitting in—which usually means knowing the lingo and procedures of whomever you're trying to trick. For example, calling a non-published number to get a flunkie and then saying "Hi it's Bob from Field Group 9, I'm over at Sector 13C doing maintenance on a 27B stroke 6 and I need passcode authorization on the sec node to run some diagnostics" might work because the flunkie isn't going to expect an outsider to call that number and know what Field Group 9, Sector 13C, or a 27B stroke 6 is, so there's an air of authority to the request.

## RIGGER TRICKS

While properly a subset of hackers, riggers have unique hardware, software, and subcultural ideologies and literature surrounding them. Most riggers are typical gearheads, more interested in drones and vehicles—the hardware and the wireless communication protocols—than the virtual environment those aspects support. That doesn't mean they ignore what's happening in the rest of the Matrix; they can't afford to. Malware and spoofing are two of a rigger's worst nightmares.

• Hackers and riggers might be the same genus of computer criminals, but they're very different breeds, and each one has their own exploits. Still, it pays for hackers and riggers to be aware of what the other side can do, if only to keep an eye out for their exploits and figure out how to counter them—or be able to use them if the situation calls for it. Hacking a rigged security system isn't all that different from hacking a node.
• Turbo Bunny

• Well, it *is* hacking a node. A node where the spider usually has his attention divided between a couple dozen devices, but a node all the same.
• Pistons

### Jacking Biodrones and Cyborgs

While the so-called biodrones and cyborgs aren't things the average shadowrunner is likely to run into, most riggers are at least aware of them. Both of these "drones" (and I use the term loosely) are rigged, so it follows that they can both be jacked. The easiest way to jack a biodrone is to intercept the traffic between it and its handler, and then spoof commands and jam it to prevent it from receiving any further orders.

• Are you speaking from experience, or is this all theoretical? Because I think most people would notice if they lost a biodrone, and even then you'd have to stop jamming it at some point to give the thing more commands.
• Rigger X

• I did it once as I described it—waited for the thing to get out of its controller's range and then did some more serious hacking to erase the owner's traces. I think certain interfaces might make the biodrone more resistant to hacking, but I haven't confirmed that.
• Pistons

You can also—though I don't recommend this—try to hack the biodrone's implants directly and work your way up to taking control of it from there, but I don't know many people that want to get within three meters of an active biodrone.

Cyborgs may also be jacked, but in this case the rigger is setting their abilities against a skilled hacker. As a cyborg is little more than a drone with an integral rigger, it becomes straight-up cybercombat in many cases. The obvious point of entry is the cyborg's integral commlink—perfect for sending spoofed commands or hacking the cyborg's drone body wirelessly, which you can be damn sure the cyborg is going to resist. In the direst situations, I imagine a cyborg could turn off its commlink, but I've never heard of that happening. You could also try and jack a cyborg body during its maintenance downtime, though your timing would have to be pretty exact, and the security on cyborg facilities is nothing to sneeze at.

### Jamming on the Fly

Sometimes you just don't have the right tool for the job, and you have to do the best you can with what's at hand. Jamming on the fly is when you *really really* need a jammer and you don't have one—but you do have a commlink, or a radio, or something that you can program to spit noise into the other rigger's bandwidth. Like most techniques, jamming on the fly is somewhere between a science and an art; more often than not it's a last-ditch effort in a non-ideal situation, and by definition you're not going to be using the preferred equipment to get it done.

• Can be effective, though. I once took a radio station in Kentucky hostage for thirty minutes to jam the comms on a military base three klicks away. They liked me so much they asked me to do a regular show, but I had to make my getaway before the black copters came for me.
• Kane

## EMP

An electromagnetic pulse (EMP) is a magnetic field in an intense state of flux traveling from a central point; when the field passes through an electronic device (like a power system or the lasers that read your optical chips), this can produce extreme voltages and dangerous currents that can burn out components or damage hardware.

The popular conception of an electromagnetic pulse as an unstoppable ultra-weapon that can send metahumanity back to the dark ages of steam power and internal combustion engines are mostly the product of the media. Optical electronic devices are mostly immune to EMPs, and our protein and optical storage media is completely able to withstand them. Don't believe the sim that the huge EMP using the Eiffel Tower as an antenna is going to wipe every commlink and datachip in France. At the very worst, it'll probably just fry the power linkages or the antenna, and you can swap those parts right out.

EMPs are generally the result of certain weapons and devices, like nukes, that you're not going to have to deal with. Or if you do have to deal with the big bombs, the EMP is slightly less important than the megadose of radiation, heat, and oh yeah that shockwave that's about to pummel you. Devices that just produce an EMP and nothing else are a lot more popular than nukes these days, though they're still covered by several multinational and multicorporate agreements. Runners may encounter EMPs through EMP grenades, HERF weapons, thunderbirds, or the Pulse spell.

Just to make it clear, you're never going to *see* an EMP. They aren't flashes of light or slowly expanding spherical energy waves like you see in anime. An EMP lasts for all of about a second, is completely invisible, and unless you've got cyberware you probably won't even feel it. What you can bank on is that it will completely disrupt all wireless and radio communication for a brief moment, and it can burn out unshielded electronics—not optical electronics, but the parts with actual bits of metal.

• I heard that if you have a cortex bomb and you're dead center when an EMP goes off, it'll fry the bomb without going off. Truth or not?
• Black Mamba

• Might work, if the cortex bomb shorts.
• Beaker

• Then again, the cascading voltages and currents caused by the EMP might set off the explosive, or the cortex bomb might go off at the cessation of a signal, in which case it's been nice knowing you. However, most cortex bombs are sufficiently well shielded (especially if they're inside a cyberskull) that it's a non-issue.
• Butch

The best protection from an EMP is inside a Faraday cage—roughly any space that is completely surrounded by solid metal or a metal wire mesh. I hear tell some corps and military groups are playing around with nanotech suits that work as well, but I've never seen or heard of one working.

# GAME INFORMATION

*The Hacker's Handbook* is designed to give player characters more options for using the Matrix with their games, expanding the opportunities for both hackers and non-hackers to interact through the Matrix. The rules and material presented in this chapter can add depth to a campaign, making shadowruns more challenging and rewarding for clever players and gamemasters.

## BUYING A BETTER HACKER

Not every character is cut out to be a hacker, and not every hacker has the time and Karma to be the best in every possible corner of the Matrix. There's no shame (well, okay, maybe a little) in paying another hacker to do what you can't do, or what you could do if you had the time and equipment. What follows below is a list of common services hackers are hired to perform and the usual street costs and availability for them. A hacker player character looking to do a little freelancing in the downtime between runs might look for some of these jobs herself.

### Anonymization

When somebody in 2070 wants to call a friend, he simply dials his friend's commcode. The commlink then connects to the MSP that issued the commcode and retrieves the access ID of the receiver. Using that access ID, it establishes the data request connection to the commlink receiving the call. In this process, the receiving commlink is aware of the access ID of the sending commlink (see *Data Exchange,* p. 53).

Anonymization services work as mediators between the two participants of a commcall or any other data request. The data package is received by the anonymizing node and then forwarded to the receiver using the anonymizer's access ID as sending ID (see *Proxy Servers,* p. 104). A trace will not reveal the access ID of the original sender, but rather the access ID of the mediator. To retrieve the real access ID, one must hack the proxy server node. If multiple proxy servers are used, each must be hacked.

### One-Time Commcodes

Some shadow MSPs offer one-time disposable commcodes—commcodes sold in advance that, once activated, can be used only once (for a single message or call). As soon as the call/message ends, all record of the commcode and the access ID that used it are securely deleted. Any attempt to track it will lead to the MSP's node (one of many that are unadvertised and changed often), but even if this node is hacked no data trail to the original caller can be found.

### Numbered Credit Accounts

Characters who are looking to keep their financial transactions confidential may take advantage of a numbered credit account offered by numerous grey and black-market Matrix banks. These institutions promise complete anonymity and confidentiality; all account transactions are handled via account number, an account code name, and heavy encryption. Though often pressured by governments and megacorps for facilitating money laundering and tax evasion, these banks are usually reliable at deflecting law enforcement.

### One-Time Credit Accounts

Like numbered credit accounts, one-time accounts are arranged as a single deposit and single withdrawal, completely confidential and with all records of the transaction immediately erased.

### Escrow Accounts

Escrow services, also offered by shadow Matrix banks, act as a secure middle-man between two parties who don't trust each other—such as a runner team and Mr. Johnson. The escrow service holds on to one party's credit (or sometimes, goods) until the other party completes its part of the deal to the first party's satisfaction, then sends the held money/goods on to the second party. If either party fails to follow through on their end of the bargain, the es-

| Hacker Services | Availability | Cost |
|---|---|---|
| Hacking a passcode | 12R | Hacking skill x 500¥ |
| Setting up a hidden account | 16F | Hacking skill x 1,000¥ |
| Copying a certified credstick | 24F | Half the amount (in real nuyen) |
| Spoofing a lifestyle (1 month) | 16F | Half cost of lifestyle for 1 month |
| Jacking a vehicle or drone | 8R | Hacking skill x 200¥ |
| DOS attack on an individual (1 hour) | 8F | Hacking skill x 200¥ |
| Tracing a datatrail | 6R | Hacking skill x 100¥ |
| Renting a botnet | 10F | Number of bots x Cost of bots x 0.5¥ an hour |
| Buying a botnet | 15F | Number of bots x Cost of bots x 5¥ |
| Anonymizing proxy service | 4 | Number of reroutes x 10¥ per day |
| Anonymized commcode (calls/messaging) | 4 | Number of reroutes x 5¥ per day |
| One-time disposable commcode | 4 | 10¥ |
| Numbered credit account | 4R | 100¥/month |
| One-time disposable credit account | 6R | 10% of the deposited amount |
| Escrow service | 8R | 10% of the deposited amount |

crow service holds on to the money/goods, eventually returning them if the deal falls through.

## PIRACY

The Cracking Copy Protection table has suggested thresholds for copying protected software. Illegal software, however, be it home-coded hacking utilities or a copy of a cracked program, has difficulties all its own. Programs in the Sixth World are constantly changing to keep up with the cutting edge of technology, and periodic patches and updates are the norm rather than the exception. Unfortunately, these patches and updates are only for legal purchasers and licensers of the program—or in the case of hacker software, may not exist at all—and without them a program slowly slides into obsolescence. A hacker can stall this degeneration either by fixing the code herself, finding the patch or update somewhere else on the Matrix, or by simply downloading a newer, updated version of the same program. (See *Legal vs. Pirated Software,* p. 108.)

### CRACKING COPY PROTECTION

| Program Type | Threshold (Interval 1 hour) |
|---|---|
| Common | 9 + Rating |
| Hacking | 13 + Rating |
| Agents/IC/Pilot | 13 + Rating |
| System | 10 + Rating |
| Firewall | 13 + Rating |
| Autosoft | 12 + Rating |

### Finding Pirate Networks

A regular Data Search on the open Matrix never reveals where a hacker can download a rated program or its updates patch for free, where a runner might find the detailed AR schematics for the latest wiz tech toy, or where the drivers for that used piece of cyberware are. Within minutes of such information being posted, law enforcement hackers appear in the node to investigate all such claims and trace and arrest whoever is making the claims or offers. However, with a little work a hacker can gain access to the peer-to-peer file sharing networks of the Cracker Underground (see *Virtual Private Networks*, below), where she can find and download programs for a nominal fee.

Finding and getting access to an appropriate network requires an Extended Data Search + Browse (8, 1 day) Test. Once connected to such a network, the character doesn't need to find another one unless the network gets shut down, or if it doesn't have the program she's looking for (both at the gamemaster's discretion).

### Downloading Programs

Once a character has made contact with the Cracker Underground, he can start looking for something to download. To find a specific program on the file sharing network, make an Extended Data Search + Browse (Availability + Desired rating, 1 Combat Turn) Test. Downloading the program to your commlink or terminal costs 10 percent of the street price of the program (see *Programs*, p. 232, *SR4A*). A glitch on the Search Test indicates the program is not on the network, and the hacker must find another network and try again; a critical glitch indicates the character has downloaded a bogus program infected with one or more viruses.

Program updates and patches are also available on underground file sharing networks and may be located in the same way. The cost for program patches and updates (which restore the degraded program to its full rating) is 10 percent of the difference in street cost between the program's current (degraded) rating and its full rating. All programs, updates, etc. from an underground file-sharing network have their copy protection cracked, if they ever had any to begin with.

## VIRTUAL PRIVATE NETWORKS

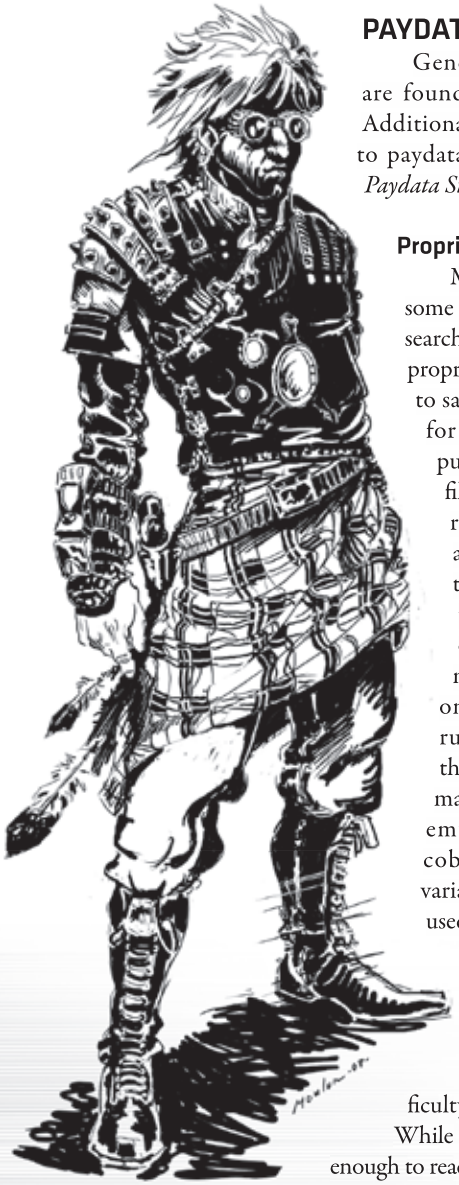
A virtual private network (VPN) is an unrated peer-to-peer program that allows users to communicate and share files and information on a less-than-simsense level, typically no more than just another window in AR or VR, and as such not counting as a connection to a node in terms of subscription lists unless they are encrypted. Networks of this kind exist for many purposes, from simple mobile social software (MoSoSo) designed to keep members of a social group in touch to pirate networks trading cracked software and liberated data.

Security for VPNs varies considerably, from secretive, passcode-protected, and encrypted networks on the one end to completely open networks on the other. Generally, VPNs depend on anonymity as much as anything else to protect them, as their most vulnerable points are the users logged on to them. Spotting a hacker using a VPN requires a Simple Action to Observe in Detail (see *Observe in Detail*, p. 147, *SR4A*) and a successful Opposed Test, rolling Computer + Analyze against the target's Firewall + Stealth. If you determine the target is connected to a VPN, you can attempt to Intercept Traffic (see *Intercept Traffic*, p. 230, *SR4A*). Secure and secretive VPNs are almost always encrypted communications.

Rarely, a virtual private network may make use of a node to facilitate real-time face-to-face communications, or as a common dropbox to dump files that other users may access and download or annotate later. Such nodes are usually in out-of-the-way corners of the Matrix and almost always hidden, requiring the user's VPN passcode to access. A node makes a VPN very vulnerable as it often contains the commcode and passcodes of all members of the network, and networks that make use of them often change nodes on a regular basis.

### PAYDATA STREET COSTS

| Situation | Cost Adjustment |
|---|---|
| Data is damaged, but mostly salvageable | –20% to –50% |
| Data is only available on an obsolete medium | –20% |
| Data is publicly available but obscure | –10% |
| Data is in a Proprietary File Format | +10% |
| Certified data | +50% |
| Sole remaining copy of data | +100% |
| Unique enchantment formula | +200% |
| Nanoschematics | +400% |
| Spirit formula | +400% |



## PAYDATA

General rules for fencing are found on p. 312 of *SR4A*. Additional modifiers that apply to paydata can be found on the *Paydata Street Costs* table.

### Proprietary File Format

Megacorporations and some national military and research institutions make use of proprietary file formats (PFF) to safeguard data not meant for release to the general public. The programs and files in PFF are for internal release only and typically are only compatible with that megacorporation's specific software or operating systems, meaning a character can only open PFF files or run PFF programs from the same corporation that made their OS. Specialist emulator programs (or cobbled-together hacker variants of the same) can be used to open or run PFF files or programs on other OSs, with minimal data loss. Treat this program as a patch in terms of cost or difficulty of acquisition.

While a company-specific OS is enough to read a PFF file, hackers need to activate the correct software modules in the OS to create or edit a PFF file. If the character has a valid corporate SIN that matches the maker of the OS, this requires a successful Logic + Software Test; a character without a valid corporate SIN requires a successful Hacking + Edit (3) Test.

*Pistons has downloaded a PFF datafile from a Renraku system. Unfortunately, Pistons is running Novatech Navi as her OS and can't read the file directly. Normally she would have to find and download a Renraku PFF reader program, or else write her own. Thankfully, Pistons still has an older commlink running Renraku Ichi—she can just send the file over to that commlink and read it from there. Of course, if she wants to edit a few details and save it, she'll have to activate the software modules first.*

### Certified Data

Matrix users can choose to certify any file by burning it to a certified datachip; all other copies of the file on the user's system are deleted automatically during this process. Certified datachips include an integral log of when a file is created, accessed, copied, and edited. This log is carried over to any copy of the data made from the certified datachip. Attempting to edit the log typically corrupts the data irreparably.

The log on a certified datachip can be wiped without corrupting the data with a successful Hacking + Edit (4) Test.

## THE FORGER'S ART

Since nuyen in circulation are constantly being tracked and monitored, the only way to counterfeit nuyen is to copy an existing certified credstick. This requires a certified credstick with a positive balance, an empty certified credstick (called a *blank*) of the same type in which to place the illicit cred and an Extended Forgery + Edit Test (see the *Forgery Table* for Interval and Threshold). For every 5,000 nuyen or part thereof the character is attempting to counterfeit, apply a 1 die penalty to the Forging Test.

*Kat o' Nine Tales has a certified credstick for 6,000¥ and decides to copy it. A visit to her local and above-board bank gets her a blank, and she connects the two credsticks to her commlink and gets to work. Kat has Forgery 3 (Credstick Forgery +2) and a Rating 4 Edit program, and she receives a 2 dice penalty for the amount of nuyen on the credstick, so she rolls seven dice. She decides that the rating of her forgery will be 2, making the threshold 48. In twenty days, Kat manages to accumulate the hits she needs and now has two certified credsticks: one with 6,000¥ in real nuyen, and a Rating 2 forgery with 6,000¥ in fake nuyen.*

When the character attempts to transfer the counterfeit nuyen (either to an online bank account or when making a purchase), make an Opposed Test between the rating of the counterfeit nuyen and the rating of the verification system (typically 1–6). If the counterfeit wins, the system accepts it as genuine; if not, it is immediately flagged as counterfeit, the transaction aborts, and local authorities are alerted. Ties are ruled in favor of the verification system.

*Kat uses her fake credstick to pay her 300¥ bar tab at Aces. The rating of the forgery is 2, and Aces has a Rating 2 verification system. Rolling for her character, Kat's player scores a 3 and a 6; the gamemaster rolls a 2 and 4 for the verification system. Looks like Kat's faux cred passes ... this time.*

### FORGERY TABLE

| Forgery | Threshold | Interval |
|---|---|---|
| Fake Corpscrip | (Rating x 20) | 1 day |
| Fake Game Credits | (Rating x 16) | 1 hour |
| Fake License | (Rating x 16) | 1 hour |
| Fake National Currency | (Rating x 18) | 1 day |
| Fake Nuyen | (Rating x 24) | 1 day |
| Fake SIN | (Rating x 32) | 1 week |

Urgent Message...

### COUNTERFEITING OTHER CURRENCIES

There are other kinds of electronic money in the Sixth World besides nuyen, and hackers can counterfeit those too. Typical examples include national currencies (UCAS dollars) and corpscrip (Aztechnology corporate pesos). These monies are usually easier to counterfeit than nuyen but are much more difficult to pass as authentic (verification systems get +4 dice on Opposed Tests to detect counterfeits). Player characters can also generate game currencies such as those used in Matrix games to buy virtual equipment (pikucredu); game cred can be purchased with nuyen inside the game but cannot (legally) be exchanged for nuyen after purchase.

A very few backward places in the Sixth World even rely on physical mediums of exchange in the form of coins or bills (see *Using Forgery,* p. 134, *SR4A*).

#### Optional Rule: Forging SINs and IDs

Creating a fake system identification number (SIN) requires extensive resources that most shadowrunners just don't have; the forger must generate and insert corroborating data into a number of government and corporate databases, the names and addresses of which are not available to the general public. The fixers and syndicates who deal in false SINs and IDs have established channels and contacts that work in the issuing institutions and have multiple backdoors into the necessary databanks. Even then it can be a tedious, expensive process to produce a high-rating false SIN, and also a very personal one involving increasing degrees of personal information and biometric data depending on the rating of the fake SIN. Solo hackers and technomancers can forge their own SINs, but without the apparatus of contacts and backdoors in place the process is much longer and more difficult than buying a fake SIN. Gamemasters should think very carefully before allowing their player character hackers to dabble in forging SINs, as it can prove unbalancing. The following rules are for use at the gamemaster's discretion.

Creating a fake SIN or fake license (see *Legality,* p. 313, *SR4A*) requires Matrix access (through a commlink, terminal, or a technomancer's innate ability) and an Extended Forgery + Edit Test (see the *Forgery Table,* p. 95, for Interval and Threshold). Fake SINs and licenses have a rating from 1 to 6 that determines how well they stand up to verification systems (see *Fake ID,* p. 267, *SR4A*). Once created, the fake SIN or license and its corroborating data must be accepted by official databases, which requires a series of system intrusions and Hacking + Edit (System, 1 hour) Extended Tests on challenging nodes; the gamemaster decides on the target system ratings and can choose to play these out or summarize them quickly with an Extended Hacking + Edit (Rating of fake SIN x System, 1 hour) Extended Test.

#### Burnt and Stripped SINs

When a SIN is exposed as a fake or is no longer usable because of crimes connected to it, it is said the SIN is *burnt*. A SIN contains biometric and identifying data that a character doesn't want to fall into the wrong hands, and can only be *stripped* of such incriminating data. Fixers and fences who buy fake SINs (see *Fencing Gear,* p. 312, *SR4A*) typically strip them automatically, but some characters might not want to take the chance that their personal data is recorded first. A character can strip a SIN with a series of system intrusions and Hacking + Edit (System, 1 hour) Tests on challenging nodes; the gamemaster decides the target system ratings and can choose to play these out or summarize them quickly with an Extended Hacking + Edit (Rating of fake SIN x System, 1 hour) Test.

When a SIN is burnt or stripped, the character loses all online accounts, licenses, DocWagon contracts, rental agreements, deeds for property, and legal debts tied to that SIN.

#### Optional Rule: Forging Passkeys

A passkey (see *Passkeys,* p. 64) contains an encrypted code that, combined with a valid passcode, allows a user access to a system. The encrypted code is incremented or scrambled every time it accesses the system, which means the code changes with every use. A dedicated character could forge a copy of a passkey, but it would require at least a schematic of the passkey and a copy of its firmware. The forged passkey (if made correctly) would be good for one use only—and it would have to be used before the actual passkey is used, or the code won't work. If someone uses a forged passkey to access an account, the original passkey no longer functions correctly, and spiders or admin users will know that the last time the account was activated, it was done with a forged passkey.

Given these limitations, most shadowrunners choose to steal or "borrow" passkeys; especially more advanced nanotech and alchemical passkeys, which require special facilities and equipment to manufacture.

## EXPLOITS

Not to be confused with the Exploit program, an exploit is a loophole, a code flaw, or other software error that a hacker can take advantage of (in other words, an exploit is what the Exploit program is designed to find, from a built-in database of security flaws, and take advantage of). A hacker that discovers a new exploit (i.e., one that software and security vendors don't know about and haven't plugged yet, and that hasn't even circulated through the hacker underground) has a decided advantage when dealing with the subject of that exploit. The hacker gains a +2 dice pool modifier for a Hacking or Cybercombat Test targeting that specific exploitable software (a particular brand of agent, program, firewall, or operating system).

Finding a new exploit requires research into the already existing exploits available for that piece of code and detailed analysis of the code itself, while also requiring a successful Extended Logic + Hacking (10 + rating, 1 day) Test. Every time the new exploit is used, there is a chance that the exploit is plugged and no longer works—the hacker won't know for sure until they try to use the exploit and it fails.

Exploits aren't restricted to a single system, so even if an exploit is plugged in one system, there's a chance it will still work on other systems, until news of its existence spreads at least. Known new exploits are always plugged when a new patch arrives for the software.

*Pistons is researching the NeoNET Aegis-II Armor program (a Rating 2 armor program). She rolls her 4 Hacking dice and 4 Logic dice against a threshold of 12; in six days she has discovered a new exploit that applies to that particular program. Pistons will enjoy a 2 dice bonus to her Cybercombat Skill Test to crash that particular armor program.*

## HACKED ACCOUNTS

Just because a hacker has bypassed a Firewall once doesn't mean he has an open pass to access the node whenever he pleases, or that he can share that access with all of his hacker buddies. Several factors must be taken into consideration first (each subject to gamemaster review).

If a node has been hacked on-the-fly, the hacker has found some gaping hole in the system security that allows him to access an account on that node. The hacker has not actually acquired the passcode for the account, however, and the exploit is likely to be noticed in a security audit and/or patched in the immediate future. This means that if the hacker wants to access the node again, he will have to hack in again. There is no way for the hacker to share the hacked account with another hacker or Matrix entity, even while the hacker is accessing the account.

If the target node was carefully probed before the hack, however, there is a better chance that the hacker can use the same method to regain access at a later point. Either the hacker has ascertained a passcode that will allow him to access the account legitimately in the future, or he has discovered a re-usable exploit (p. 96)—the gamemaster determines which. In either case, this access may be shared with others, allowing them to use the account or re-usable exploit. Eventually, however, passcodes may expire or be changed, and exploits may be discovered and patched. Nothing lasts forever.

No matter how access was obtained, if a hacker triggers an alert, their method for accessing the node will likely be closed off in the future, to prevent future intrusions.

Hackers may of course make arrangements while within a node to ensure that they can access it at a later point. Options include inserting a re-usable exploit, creating a "legitimate" account, or creating a hidden account or access point. These methods are referred to as *backdoors.*

## BACKDOORS

A backdoor is a means for a hacker or technomancer to gain repeated access to a node with less effort than hacking their way in every time; this means it is typically hidden from the site administrators, though in the case of repeated use of legitimate accounts this might mean hiding in plain sight. Before leaving a node they're likely to come back to, some hackers will take the time to code in an account or exploit that will let them access the node again. In general there are four types of backdoors: reusable exploits, legitimate accounts, hidden accounts, and hidden access points.

### Reusable Exploits

As noted under *Probing the Target* (p. 236, *SR4A*), some probed exploits may be used repeatedly if the hacker doesn't do something to give them away or it they aren't discovered. The drawback to this "open hole" sort of backdoor is that the system gets an Analyze + Firewall Test every time you use it.

Hackers who have hacked their way into the node can also create their own reusable exploit; a specially crafted flaw in the node's firewall that allows those who know about it to hack the node with extreme ease. Creating a reusable exploit requires a successful Extended Software + Exploit (Firewall + System, 1 Initiative Pass) Test if you have at least security-level access on the node—otherwise replace Software with Hacking. Once created, this provides a hidden exploit that gives the hacker a +6 dice pool modifier to gain access to that node using the Exploit program.

The details of a known exploit like this may also be traded/sold to other hackers, who will also receive the +6 dice pool bonus until the exploit is discovered and removed (see *Detecting Backdoors,* below)

### Legitimate Accounts

Nodes expect a certain amount of traffic from normal users, and for many work-related nodes even some off-hours access from home or private terminals is typical or expected. A hacker who steals the passcode to a legitimate account can, with care, continue to make use of that account for some time before a spider notices anything, if they ever do.

A hacker who has hacked the node may also create a "legit" account on the system (see *Hacking*, p. 235, *SR4A*) and then hide the fact that they created it. This requires a successful Software + Editing Test if you have at least security privileges on the node, or a Hacking + Edit (2) Test if you do not. For security-level access, increase the threshold to 3; for admin access, increase it to 4. New accounts of course show up on security audits and are usually carefully scrutinized for legitimacy. All of the account's actions are also logged—it's not hidden, as it was created with the façade of a legitimate account. A verifiable account on a corporate system combined with a fake SIN and/or records that the hacker is employed by that corporation can make a very convincing cover story for an infiltration.

### Hidden Accounts

A hidden account is not visible to spiders or administrators, being discernible only by the system. While this account allows the hacker to access the node freely, it is still subject to account privilege limitations and spiders who perceive the character will assume them to be trespassing as they will not appear to have an account.

To create a hidden account, you must already have access to the node (either legit or hacked) and must follow the procedure for creating a legitimate account noted above. On the next action, the legitimate account must then be hidden with a Hacking + Stealth (Firewall, 10 minutes) Extended Test. As with any other account, this hidden account has a unique passcode; anyone with that passcode may access that account. Previously existing legitimate accounts may also be transformed into hidden accounts this way, but the access log must also be modified or a security audit will show an account mysteriously disappeared.

### Hidden Access Points

A hidden access point is similar to a reusable exploit, except the hacker exploits a software flaw that allows him access to a node

without actually granting him an account. To create a hidden access point, the hacker must have previous access to the system and must make a Hacking + Exploit (Firewall + System, 1 minute) Extended Test.

The advantage is that such hidden access points make it very easy to penetrate the system, requiring only a simple Hacking + Exploit (1) Test, and the Firewall gets no test to detect the intruder. As no account is being used, access won't be noticed as long as the intruding hacker remains under the radar of patrolling IC.

Since no passcodes have been obtained, however, the hacker has no account privileges at all and must rely on Hacking for all tests as long as he is connected to the node in this manner (it is common practice to access the system via the hidden access point and then create an account, leave the system, and do a "legal" log on with the fake account). IC or security hackers that perceive the hacker will immediately recognize him as an intruder.

Note that the actions of a hacker who uses a hidden access point are still recorded in the access log, but they are obscured and confusing because they are not tied to an account. The hacker's datatrail may still be tracked, however.

### Detecting Backdoors

Users with security or admin privileges can conduct account audits and security sweeps to look for known or suspected backdoors. Of course, hackers with security or admin access to a node can conduct their own searches and keep the results to themselves, making use of the hard work of their fellow hackers. Some technomancer hackers have been known to watermark their backdoors (see p. 243, *SR4A*), so that other technomancer or sprite hackers can find them.

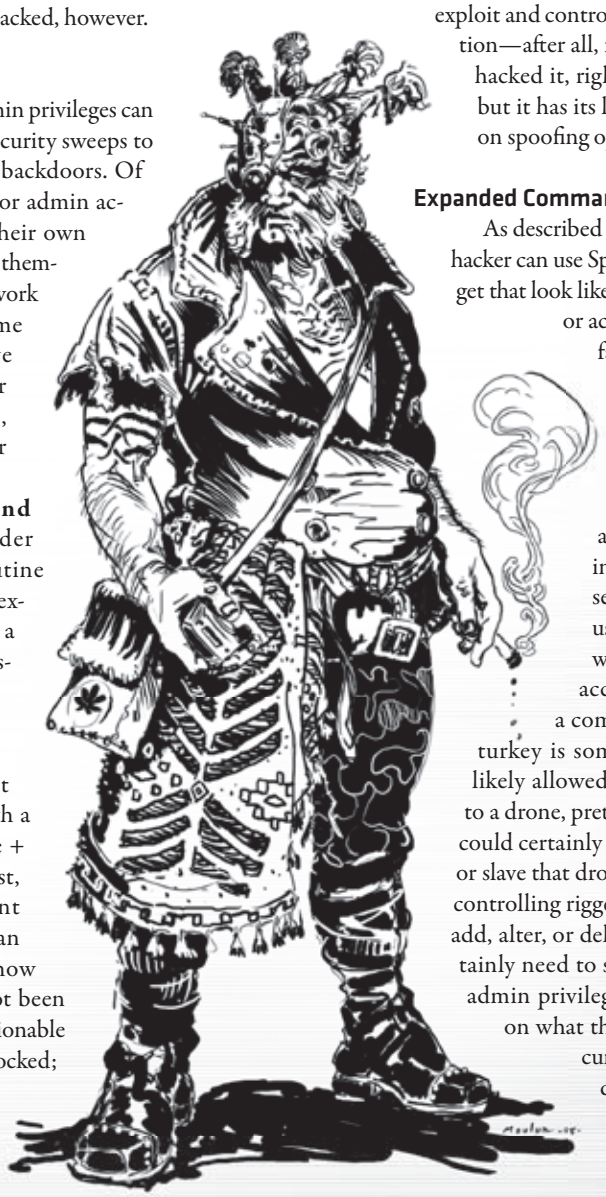
**Reusable Exploits and Hacked Accounts:** A spider or hacker conducting a routine audit will detect a reusable exploit or unauthorized use of a legitimate account on a successful Extended Data Search + Browse (lowest Stealth rating of hacker using exploit or account, 1 day) Test; the exploit may be immediately fixed with a successful Extended Software + Edit (Firewall, 1 minute) Test, while the legitimate account is typically locked pending an official review. If the logs show the legitimate account has not been engaging in any illegal or questionable activity, the account will be unlocked; otherwise the user will face arrest and/or questioning. Hacker-created accounts subject to this review are typically deleted unless the hacker has taken care to have a good cover story and has been editing the logs to hide her activities.

**Hidden Accounts and Access Points:** Hidden accounts and access points do not show up on routine inspections by security-level and admin users, but if a spider becomes aware of them (either through a sloppy log edit or seeing the hacker use them), a thorough account audit—a successful Extended Data Search + Browse (lowest Stealth Rating of hacker using access point or account x 2, 1 day) Test—will reveal them, after which they may be edited or erased as normal.

**Probing the Target:** At the gamemaster's discretion, a hacker who is probing the target (p. 236, *SR4A)* may discover a backdoor rather than a flaw to exploit.

## ADVANCED SPOOFING

The *SR4A* rulebook details several good uses for the Spoof program: redirecting traces, spoofing the datatrail, and spoofing commands to agents, drones, and sprites. A common misconception is that spoofing is a simplified version of hacking in with an exploit and controlling the agent, drone, or device in question—after all, if the target does what you want, you've hacked it, right? Not really. Spoofing is a great tool, but it has its limitations. The following rules expand on spoofing options and provide a few new ones.



### Expanded Command Spoofing

As described under *Spoof Command,* p. 232, *SR4A,* a hacker can use Spoof software to send commands to a target that look like they were sent by someone with control or access privileges. This trick may be used to falsify commands to drones, agents, sprites (technomancers only), electronic devices, and slaved nodes.

Spoofed commands will seem to come from the authorized user you are spoofing (why you need their access ID), and so will be treated as having the same access privileges (personal, security, or admin) as that impersonated user. It is up to the gamemaster to decide what commands are legitimate for which access privileges. For example, spoofing a command to an oven to start cooking the turkey is something anyone accessing the oven is likely allowed to do. If you are spoofing commands to a drone, pretending to be the controlling rigger, you could certainly instruct the drone to log that rigger off or slave that drone to your commlink instead (since the controlling rigger would have privileges to do that). To add, alter, or delete an account, you would almost certainly need to spoof a command from someone with admin privileges. Many legitimate users have limits on what they can do with their accounts, and security- or safety-conscious spiders can and do program agents, drones, and nodes to ignore certain orders. After all, the last thing a security hacker wants is to be the target of their own IC.

Spoofing commands from a user with security or admin privileges is more difficult, just as is with hacking in and obtaining an account with such privileges. Apply a dice pool modifier to the hacker for the Opposed Test equal to –3 for spoofing security privileges or –6 for spoofing admin privileges.

Spoofing commands for actions that are illegal for those access privileges is simply not possible. To bypass access restrictions, you have to hack in.

Note that a hacker can only spoof one command at a time, and only if she has the access ID of a legitimate user (see *Spoof Command*, p. 232, *SR4A*). Once a command is sent, she has no control over that agent, drone, or node until she spoofs the next command. If your hacker needs to give multiple commands—or tells the target to do something that a legitimate user can't order it to do—you're much better off hacking the node than spoofing commands one at a time.

### Spoofing a Datatrail Online

Since nodes require an access ID before they will allow a connection, it is important to spoof your datatrail (if you are so inclined) *before* you actually access other nodes. Once you have logged onto other nodes, a change in access ID will automatically close your connection to other nodes—after all, you are no longer who you said you were. Under some circumstances, this may be an expedient way of closing multiple connections. For example, if you are under attack by Black IC in another node, you can try to spoof your datatrail in order to change your access ID and log off that node. If the Black IC is jamming your connection, however, this will require an Opposed Test pitting your Hacking + Spoofing versus the Black IC rating + Response.

You can also use this trick to try and avert a direct trace. If someone is using Track to trace you, you can spoof your datatrail and change your access ID as normal. While this will sever all of your connections, it means that the Track will only be able to trace you to the nearest node that your connection happened to have been routed through. The tracking hacker can still acquire your old access ID, but will not be able to pinpoint your exact physical location—though he will know that you are close to that nearest node.

**SPOOFING LIFE**

| Lifestyle | Threshold |
|---|---|
| Squatter | 2 |
| Low | 4 |
| Middle | 12 |
| High | 48 |
| Luxury | 100+ |
| Hospitalized Standard Care | 15 |
| Hospitalized Intensive Care | 30 |

### Spoofing Life

A hacker can improve her lifestyle to a given level for one month by making a Hacking + Spoof Extended Test. See the *Spoofing Life* table, p. 99, for threshold; the interval is 1 day. For a hacker living on the streets, this equates to making vending machines give out free eats and opening locked doors to utility sheds and bathrooms for them to sleep in. For anyone else, it means redirecting automated bill payments or telling utilities and services that the hacker is a subscriber. A character can make multiple tests to improve their lifestyle more than once during a given month.

*Dogbody is tired of living with his parents and decides to move out. After living on the streets for a week, he decides he needs someplace to crash and tries to upgrade to a low lifestyle. With Hacking 5 and Spoof 4, Dogbody is rolling 9 dice to meet a threshold of 4, but he glitches it on the first day and has to start over again. Two days later, Dogbody is enjoying day one of his thirty-day stay in a coffin motel while chomping down on a Gooey Bar. Life is looking up.*

### Spoofing Protection

If the hacker is facing an opponent that is wielding an offensive program with the Limitation option (p. 114), he may attempt to spoof his persona in a way that the limited program will not work against him. To do this, the hacker must be aware that the program has that specific option, via an appropriate Matrix Perception Test. He can then attempt to spoof his persona so that it appears to be something it's not. For example, a Renraku security hacker may be wielding an Attack program with a Limitation that prevents it from being used on certified Renraku personas. A hacker who has learned this may spoof his persona to appear Renraku-certified, thus making himself invulnerable to the program. This requires an Opposed Test pitting the hacker's Hacking + Spoof against the opponent's Analyze + Response.

## MASS PROBES

Sometimes hackers want to quickly obtain a list of nodes that appear vulnerable to their exploits. Mass probing functions a great deal like probing (see *Probing the Target*, p. 236, *SR4A*) but queries a large number of nodes very quickly to find the most common system flaws. Many hackers automate this process using an agent while they are offline. Mass probing is typically the first step in the creation of a botnet; after gaining access to poorly defended nodes, the hacker uses viruses or worms to infiltrate the system and set up the bots.

A Mass Probing Test is an Extended Hacking + Exploit (4, 1 day) Test. Every hit over the threshold is equivalent to a reusable exploit (see *Backdoors*, above) in five nodes; for the equivalent of a legitimate account with personal access privileges, increase the threshold by +3; if you want security-level access, increase the threshold by +9, and for admin access increase the threshold by +16. Glitches on the test indicate that one of the nodes is a honeypot (see p. 73). The gamemaster decides what these specific nodes are; more often then not they are poorly defended systems without much to offer, such as low-rating commlinks, public terminals, and minor workstations. Backdoors don't last forever, however, and every week at least 2D6 accounts are closed off in security updates or regular system audits.

Unlike regular probing, when a hacker makes the actual intrusion, the target node gets two free Analyze + Firewall Tests with a threshold equal to the intruder's Stealth program rating (or in the case of an agent or sprite, their Stealth program); this extra test represents the additional attention of spiders who might have

Urgent Message...

### HACKER BOOKKEEPING

One issue with botnets and mass probes is that player characters can quickly accumulate a *lot* of compromised nodes and a lot of bots—more than a gamemaster can be expected to fully detail at the table. The key to avoiding unnecessary bookkeeping and holding up the game is for the gamemaster to plan ahead and let the player worry about the bulk of the bookkeeping. Make up a list of five (or ten or fifteen) nodes that would be of particular interest to the hacker, are specifically relevant to the campaign, or are particularly amusing false leads; the majority of the rest of the nodes compromised by mass probing will be home terminals, student commlinks, and other nodes only useful as a place to store a bot or rip an access ID from.

logged the probe, security patches updating software in the time between the probe and the intrusion attempt, and other security measures to protect against mass probing.

Mass probing never reveals hidden nodes.

## BOTNETS

A botnet is like a specialized VPN that allows a hacker to maintain and manage large numbers of agents (or worms) without overloading her subscription list. The agents are loaded with a copy of the unrated botnet program along with the rest of their payload and loaded into separate nodes to run independently. From that point on, the agent (or bot) counts as only a single subscriber on your subscription list, and its active programs do not count toward your persona's active program limits. However, the only way to communicate with the agent is through the botnet.

The botnet program contains a list of all the agents online and connected through the botnet, with simple status symbols communicating their effective Matrix attributes, current Matrix Condition Monitor, payload, location, and what action they are undertaking. With a Simple Action, the hacker can issue a command (see *Issue Command*, p. 229, *SR4A*) to any number of bots in the botnet.

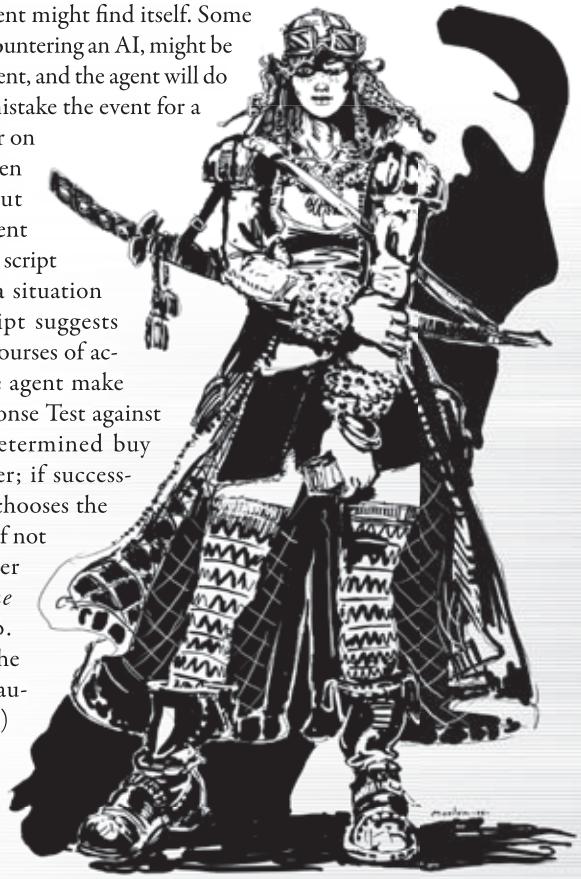
Botnets can be intercepted, hacked, or spoofed in the same manner as virtual private networks (see p. 94). A compromised botnet can quickly lead to another hacker "stealing" your bots by locking you out of your own botnet, or even turning them against you. For this reason, bots typically feature an Encrypt program that protects their communications or can be programmed to report in or shut down if subjected to an unsuccessful Spoof or Hacking attempt (player's discretion). You may also check to see if your botnet is compromised with an Opposed Test, putting your Hacking + Analyze versus the intruding hacker's Hacking + Stealth; success allows you to cut off the compromised bots and deny the intruding hacker the use of the rest of the botnet.

Botnet programs contain access IDs for their handlers, theoretically allowing others to trace you (see *Track*, p. 219, *SR4A*) back to your originating node; most hackers use proxy servers (p. 104) or disposable commlinks to negate this potential threat. Bots lack some of the independence and adaptability of other agents and have a more limited ability to communicate—usually only to signify if a job is done, if they take damage, or if someone has attempted to hack them and failed.

If a hacker is using mass probing to place bots, accounts lost to security upgrades and system audits will usually remove the bots as well. A botnet can also assist a hacker in performing a mass probe; add a 1 die positive modifier to the hacker's Mass Probing Test for every bot in the botnet carrying an Exploit program, up to a maximum bonus equal to the character's Hacking skill.

## AGENT SCRIPTS

Like IC, agents—including mooks, bots, and drone pilots—can have scripts (see *Scripting*, p. 69), a list of actions that they take when certain conditions apply. Scripts can make a hacker's (and a gamemaster's) life much easier, as hackers can spend less time micromanaging their agents or bots. Players and gamemasters should be aware that no script—no matter how ridiculously long, complex, or detailed—can handle every situation in which an agent might find itself. Some events, like encountering an AI, might be without precedent, and the agent will do nothing—or mistake the event for a different trigger on the script. When in doubt about whether an agent should follow a script or not (or in a situation where the script suggests two contrary courses of action), have the agent make a Pilot + Response Test against a threshold determined buy the gamemaster; if successful the player chooses the agent's action, if not the gamemaster does (see *Issue Command*, p. 229, *SR4A*). The Adaptability autosoft (p. 113) may aid in this test.



| Mook | Cost Multiplier | Availability Modifier |
|---|---|---|
| Unrestricted Agent | 1.2 | +2 |

Urgent Message...

### TO MOOK OR NOT TO MOOK?

For some characters, particularly those just starting out, it may look like a better deal to invest in a high-rated commlink, OS, and an agent (the mook) to take care of all of your hacking needs. Using a mook isn't against the rules, nor is it gamebreaking, but players and gamemaster should both be aware and the advantages and disadvantages of the situation.

When mooks are used en masse, or combined with botnets, a non-hacker character could potentially maintain a small army of agents and terrorize the Matrix from the relative safety of an AR interface. Mooks aren't a perfect replacement for hackers, however, for several reasons. For starters, agents are really only adept at following orders—so-called agent scripts (p. 100)—and are not very useful at handling decisions on their own. For more details on this, see *Agent Competency,* p. 111.

Still, mooks are useful as a trained dog—just point at the target and say go. They are also inherently replaceable—one gets trashed, load up another. Even a high-rating mook won't roll as many dice as a hacker with good skills, programs, and right implants, however. As a second-string team or backup plan, however, mooks certainly make sense. Don't expect to use a mob of copied agents to gang up on a target, though, as their built-in access IDs will keep all but one out of node (see *Autonomous Programs,* p. 110).

Note that commercially-bought legal agents have built-in limitations that prevent them from taking any illegal action—broadly, this means they won't perform any action that requires a Test involving any skill in the Cracking Skill Group, even if they have the correct program loaded, though gamemasters may rule this is a much broader restriction on any blatantly illegal Matrix activity. Hackers can remove these limitations with an Extended Software + Logic (13 + Rating, 1 hour) Test, code agents without them, or buy unrestricted agents from other hackers.

The main drawback to a mook is that a character that relies on them will almost never develop their Cracking group skills and will miss out on most of the fun of Matrix.

It's worth keeping in mind that player characters aren't the only ones that could use mooks; non-player characters are as likely to use a mook if they lack Matrix skills, and gamemasters can use that to their advantage.

## DENIAL OF SERVICE ATTACKS

A denial of service (DOS) attack is a method of keeping legitimate users from accessing a specific node, or even the Matrix at large. Cutting off traffic to a specific node could be the beginning of a plan for extortion, or an effort to prevent outside reinforcements from entering a node while a hacker is busy working with it. More simply, a DOS attack can prevent someone from calling for help using their commlink or from getting directions while in their vehicle. Devices that a legitimate user cannot access are much more susceptible to spoofing because legitimate users cannot counteract the orders given them.

The central focus of most DOS attacks is a node's active account list; by editing the list a hacker can sever a connection (see *Terminate Connection,* p. 238, *SR4A*). A hacker can also instruct the node to block future access connection requests from a particular node or access ID (or a range of nodes/access IDs), locking the target out. To accomplish this, the hacker must have access to the node and must make a Computer + Edit (1) Test if they have security or admin privileges; or a Hacking + Edit (2) Test if he does not. Accounts may also be deleted (if active, the user's connection must be terminated first) with a successful Software + Editing (1) Test, assuming you have security or admin privileges; Hacking + Edit (2) Test if you do not.

There are many other ways to accomplish a DOS attack: jamming a wireless device, cutting the hardlines on a physical network, or changing the routing to prevent traffic in or out of the target node all accomplishes the same task. Causing the system to crash can also achieve the same effect, though only for the amount of time it takes the system to reboot.

### Distributed Denial of Service Attacks (DDOS)

Hackers can also use botnets (p. 100) to perform a form of denial of service attack that is generally easier to accomplish than hacking the target node directly. Even in the 2070s, nodes have limits to the number of data transfers and access requests they can handle at once, though this is rarely an issue. A hacker performing a DDOS attempts to overload the node by having a botnet flood it with traffic of all kinds.

In most cases, DDOS attacks require massively large botnets. For standard nodes, reduce the target node's Response by 1 for every System x 4 bots flooding it with traffic. A node with System 5 and Response 5, for example, hit by a DDOS attack from a botnet with 100 bots, would have its Response reduced to 0, freezing all activity on the node. Even if the node is rebooted, it will be slammed with traffic as soon as it starts again, until the DDOS attack ends.

A node under DDOS attack has three options. First, it can spoof its access ID, so that the DDOS can no longer find its target. The node must be offline (not meshed with other nodes) to switch access ID. Second, it can try to block access from botnet access IDs or attempt to filter out all flooding traffic. The success of these latter options is largely up to the gamemaster's discretion.

## MASS ATTACKS

A mass attack refers to a team of hackers pooling their resources to hack a particular system. Functionally, a mass attack is Probing the Target (see *Probing the Target*, p. 236, *SR4A*) with a Teamwork Test. Hackers and technomancers can work together on mass attacks. If the test is successful, all of the participating hackers gain access to the node.

Agents and sprites cannot participate directly in Teamwork Tests, but add +1 die to the prime character's dice pool for each agent or sprite assisting (maximum +5).

Urgent Message...

### ARMY OF CODEZOMBIES!

With botnets and mass attacks, players are probably wondering why hackers don't simply send agent after agent to hack a node. Statistically, at some point the dice will roll sixes and you'll be home free. So why waste the time and energy planning a hack?

First, bots that have the same access ID will be blocked from entering the same node at the same time (see *Autonomous Programs,* p. 110). Even if they have different access IDs, security hackers aren't stupid. While the first two or three agents might be dismissed as kids playing around or spammers trying to break through a firewall, repeated attempts (especially if the agents are identical copies or from the same node) will rouse suspicion, triggering an active alert or drawing a security hacker to investigate and possibly trace the source of the offending agents, which will be removed from the node's subscriber list and all connections between the two refused.

Brute force methods—sending a group of agents to force their way through a node in cybercombat—are rarely effective. Most nodes will quickly terminate the agents' connections and/or bring in large numbers of IC to deal with the intruders. Because they lack true intelligence, agents are usually susceptible to simple tactics like crashing the programs they are using. Once disarmed, agents are easy game for security hackers and intrusion countermeasures.

So what's the point in having massive numbers of agents on hand? Agents are handy for being in more places at once than your commlink allows, for helping with denial of service attacks, and for automating actions like mass probing and data searches. Savvy hackers prefer to see how well an agent does against a node before they put their own frontal lobes on the line trying to hack it. In a pinch, agents are also a good way to ensure you have numbers on your side in cybercombat.



## HACKER TRICKS

The following rules expand on the options presented in *SR4A* and other *Shadowrun* products on hacking, with an eye to answering lingering questions on accessing cyberware, electronics, nanites, and other devices.

### Hacking Cyberware

Not all cyberware is hackable, though enough is to make a hacker's interest worthwhile. To determine if a particular cyberimplant can be hacked, the following criteria must be met (note that these criteria actually apply to almost all devices, not just cyberware):

First, the cyberware must be computerized—not all implants need a built-in computer. Most cyberware, however is either computerized (or at least equipped with RFID sensor tags) so that it may be queried for diagnostics, controlled remotely or via direct neural interface, or communicate with other implants/devices. See *DNI and Wireless Functionality,* p. 31, *Augmentation.*

Second, the implant must be accessible by the hacker, via wired or wireless connection. Most external implants (like cyberlimbs) only have wired connections, requiring the hacker to physically jack in to access the device. A datajack provides immediate access to all cyberimplants with a direct neural interface. Many internal implants have wireless links to aid medical staff in running diagnostics (like wired reflexes) or to link to other devices (like a smartlink). The Signal rating of internal implants tends to be low (usually 0), meaning that a hacker needs to be in close range. Such implants are often slaved to the character's commlink, however, so a hacker who infiltrates the master node can access slaved implants (see *Slaving,* p. 55). Some internal implants (such as cortex bombs) have no wireless or DNI connection and so are isolated from other systems, requiring surgery to allow a hacker to jack in and access the device.

If these criteria are met, the hacker can attempt to hack or spoof the implant following normal rules. Device ratings for standard types of cyberware are given on p. 222, *SR4A*. Some implant nodes/transmissions may be encrypted for extra protection, requiring that the hacker decrypt them first (see *Encryption,* p. 65). Like other devices, cyberware can be manipulated within the limits of its programming and functionality. In most cases, such actions require no test to someone with the proper access privileges. In the case of commands that exceed operational parameters or access privileges, an Opposed Test pitting Command + Hacking Test versus System + Firewall may be required. It would take too much space to provide an exhaustive list of possibilities, but here are a few examples (players and gamemasters are encouraged to be creative when devising other options—as always, the gamemaster has final say):

- Cybereyes can be shut down or crashed to make the target blind.
- Pre-recorded or self-created (using Computer + Edit) sounds could be played within hacked cyberears to make the target hear things.
- Incriminating evidence (for example, forged smartlink footage of a shooting) could be downloaded into an implant's memory, framing the victim for a crime.
- The implant may be activated (for example, triggering foot anchor implants to keep someone from running away) or shut down (turning an internal air tank off, to force them to breathe).
- The target character may be shut out of controlling his own implants by deactivating DNI or altering the account privileges (requiring a Hacking + Editing Test).
- Seizing control of a cyberarm and using it to attack others, or even the cyberlimbed character.

### Hacking Smartlinks and Smartguns

Smartguns and smartlinks are both low-level wireless devices (Signal 0), and the default mode for smartguns is private access—a primary user account is registered when the gun is purchased, and that user can set up guest accounts for friends and allies instead of letting anyone pick up the gun and access the smartgun link and/or fire the device. To prevent their smartguns from being hacked, some users place the smartgun in hidden mode or disable the wireless access and use a skinlink or datajack located on the inside of the wrist to connect to the smartgun (the fiber optic cord also serves to make the gun easier to recover if the character drops it).

Issuing commands to a smartgun through a smartlink is a Free Action that requires no test; issuing commands to a smartgun through a commlink or any other wireless device is a Simple Action and requires a successful Computer + Command (1) Test. If two characters are attempting to command the same smartgun, make an Opposed Computer + Command Test, with the winner determining what the smartgun does that round. Some street samurai store a copy of the Command program in their smartlinks specifically for these tests.

### False Diagnostics

By default, cyberware (and other electronic devices configured for open access) provide information on the current state of the device, including the official designation and serial number for the device, the owner, the license number, the version of the operating system it is running, fuel or power remaining (if applicable), critical temperatures, malfunctions, and the date of the last maintenance, upgrade, or modification. A hacker can change some of the personal data (owner, license number) with a successful Software + Edit Test; changing any of the other information requires a Hacking + Edit Test (difficulty threshold determined by the gamemaster). In low-security settings where the guards cannot tell exactly what an implant is, a false diagnostic reading with a valid license can be enough to get the character through without too much scrutiny.


### Hacking Electronics

A character can identify an unfamiliar electronic device and figure out how to turn it on with a successful Computer + Logic Test. Once the device is powered up, characters can access it. Most devices only have a single account with admin privileges and are configured for open access—anybody can come by and use them. More complicated and expensive devices may have multiple accounts and more limited public access.

Devices generally feature wired access (requiring the hacker to physically jack in), wireless access, or both. Because most hardware devices are configured for open access, limitations are generally hardwired or preprogrammed in. Bypassing or modifying hardware limitations on a device requires a Hardware + Logic Extended Test. Refer to the *Build/Repair Table* on p. 138 of *SR4A* for the Threshold and modifiers, the Interval is usually 10 minutes (longer for larger or more complex devices, at the gamemaster's discretion). A microtronics tool kit (see *Tools*, p. 332, *SR4A*) or better is typically required.

Generally, electronics only have a single rating, the Device rating (p. 222, *SR4A*), which is used in place of all of its Matrix attributes. Gamemasters may choose to specify the Matrix attributes for particularly important device rather than rely on this catch-all. When a player character is attempting to manipulate the device within the bounds of legitimate use, they use Computer + Logic (for the general function of the device), or Computer + Program rating (if within the normal parameters but an unusual task); if the player wants to get the device to act outside of legitimate parameters, roll Hacking + Program rating.

### Hacking Nanites

Individual nanites are too small and simple to be hacked individually—or for there to be much use if you managed it—and entire nanite colonies are too complex, even for the most sophisticated swarm-rigging programs. Instead, hackers focus on accessing and reprogramming nanohives, nanofaxes, and desktop forges, or triggering and shutting down nanoware (see *Triggered and Shutting Down Nanoware*, p. 108, *Augmentation*).

Nanites cannot normally be controlled to a great extent, but hard nanite systems can be reprogrammed from their supporting nanohive. Individual nanohives can be accessed wirelessly (Signal 0) and hacked or spoofed using the standard rules (see *Hacking Cyberware*, p. 102); the hacker can then get cracking reprogramming the nanites (see *Reprogramming Hard Nanites*, p. 107, *Augmentation*). To save time, if the hacker has a sample of the nanite system and a microtronics shop, she can write the program in advance and simply upload it using Spoof.

Nanofaxes and desktop forges have extensive protections against hacking. Typically, neither sort of nanomanufacturing device connects to the Matrix unless they are expecting a software upgrade or new nanoschematics. Unlike other devices, nanofaxes and desktop nanoforges are usually as well-protected as high-security nodes with

**CYBERWARE DEFENSES**

How can a character protect his cyberware from hacking?

1.) Turn off or remove any wireless links (see p. 31, *Augmentation*).
2.) Use a direct physical connection rather than wireless (externally-accessible implants only).
3.) Keep the Signal rating low so a hacker would have to be within close range.
4.) Use a good Firewall program.
5.) Use a good Encryption program.
6.) Stay in hidden mode.
7.) Slave the implant to your secure commlink (see *Slaving*, p. 55).
8) Install Data Bomb, ECCM, or IC programs.

Urgent Message...

Urgent Message...

## A NOTE ON COMMANDING DEVICES

There's more than one way to rig a drone. The same is true for other devices controlled through the Matrix. Here's a quick and handy reference guide.

### Issue Remote Commands

You may remotely command any device that you have subscribed to your persona (p. 224, SR4A) with a Simple Action (see *Issue Command,* p. 229, *SR4A*). You do not need to be in the same node as the device, as long as it is subscribed and your command can reach them. Multiple devices may be controlled as a single subscription, but this means they all receive the same command. Nodes, devices, agents, drones, sprites, etc. may all be commanded this way.

In this case, the commanded device acts on the orders independently on its own action. Pilot + autosofts are used for any relevant tests. If the orders are complex, the gamemaster can roll Pilot + Response to see if the device comprehends them (see p. 111). More complicated orders can be issued in the way of scripts (see *Agent Scripts,* p. 105).

### Remote Control

Rather than letting the device operate on its own, you may access it directly via AR or VR, using the Command program (see *Controlling Devices,* p. 220). You must either log in to the device or subscribe it to your persona. The program provides you with a virtual interface, allowing you to control the device like a video game. Most devices have built-in Command programs, which you can run if you lack your own.

A remote-controlled device acts on your Initiative. All tests are made by you, using Command + an appropriate skill. For example, to fire a gun emplacement, you would roll Command + Automatics. To maneuver a rotordrone around a tree, you would use Command + Pilot Aircraft +/– Handling.

Devices, agents, and drones may all be remote controlled this way.

### Jump In

Your final, and most direct, option is to "jump into" the device with a Simple Action via full-immersion VR (see *Jumping In,* p. 245, *SR4A*). This is only possible with devices that have rigger adaptation (p. 348, *SR4A*), typically drones and vehicles. In rare occasions, other devices will feature rigger adaptation.

Devices rigged this way act on the rigger's Initiative, and tests are made using the rigger's skill + appropriate vehicle attribute (see *Common Rigger/Drone Tests,* p. 105).

multiple levels of access, linked passcodes or nanotech passkeys, encryption, data bombs set to activate during off-hours, and proactive IC. If a hacker does manage to access a nanofax or nanoforge, they're limited to producing items that the nanomanufacturing device that they have the correct feedstocks to produce, and has nanoschematics for. Nanofaxes are further limited in that they can only create a specific type of gear, such as personal microtronics or pistols. If a nanofax or desktop nanoforge is compromised (an Active Alert) instead of shutting down it will self-destruct. Stolen nanofaxes and desktop nanoforges are typically ordered to self-destruct wirelessly, or do so automatically when they leave the range of the wifi network of the building they are in.

Nanoschematics are kept in high-level security nodes, and legitimate users download them by logging onto the node with their passcodes and then verify their log-on by sending a valid license number that is hard-coded into the nanofax processor. The nanoschematics are encrypted when downloaded from the secure node. Provided the character has access to a nanofax, finding the license number requires a Hardware + Logic (4) Test. A nanofax license number only works with the appropriate matching account. Nanoschematics cost serious nuyen, and few show up on peer-to-peer file sharing networks (see *Piracy*, p. 94)

### Proxy Servers

A "proxy server" is a program routine that acts as a go-between, transferring data from a user (the "client") to another user or node. The advantage to proxies is that they act as an intermediary, so the data seems to be coming from the proxy rather than the client. Hackers and shadowrunners find proxies very useful both as anonymous remailers (obfuscating the original message source) and to foil tracking attempts.

Almost any node can be configured to act as a proxy server, though this typically requires admin access and a Computer + Edit (10, 1 Initiative Pass) Test to set-up (use Hacking in place of Computer if you do not have admin privileges). Once set up, messages that are sent from a client through the proxy server node will seem to have originated from the proxy node. In order to determine the source of a message, a hacker would need to trace the message back to the proxy server node and then hack that node's access log (or request it from the admin/owner of the node, if they are cooperating). Anonymizing proxy servers are often set to not keep or to delete message transfer logs.

A hacker can also route his connection through a proxy server as a means of hindering traces. This increases the threshold by +4 for Tracking Tests for each proxy server used. The drawback, however, is that each proxy server reduces the hacker's Response by 1.

### Spotting Traces

It can be advantageous to know when someone is trying to track your datatrail (see *Trace User,* p. 232, *SR4A*), so that you can redirect the trace or otherwise make haste. In order to spot a trace, you must be in the same node that the track attempt is launched in (if someone is attempting to track your datatrail from the access log of a node you are no longer in, for example, you will not know). Spotting the trace requires a simple Matrix Perception Test (1) Test. However, if the tracker is trying to keep the trace discreet, you must beat them in an Opposed Test pitting your Analyze + Computer versus their Track + Stealth.

## COMMON RIGGER/DRONE TESTS

| Action | Jumped-In Rigger Dice Pool | Autonomous Drone Dice Pool | Remote-Controlled Dice Pool |
|---|---|---|---|
| Initiative | as rigger | Pilot + Response | as rigger |
| Attack | Sensor + Gunnery | Pilot + Targeting | Command + Gunnery |
| Melee Defense | Response + Melee skill | Pilot + Defense | Command + Melee skill |
| Ranged Defense | Response | Response | Command |
| Full Defense | as above + Dodge | as above + Defense | as above + Dodge |
| Damage Resistance | Body + Armor | Body + Armor | Body + Armor |
| Infiltration | Response + Infiltration | Pilot + Covert Ops | Command + Infiltration |
| Maneuvering | Response + Vehicle skill | Pilot + Maneuver | Command + Vehicle skill |
| Perception | Sensor + Perception | Sensor + Clearsight | Sensor + Perception |

## RIGGER TRICKS

Like hackers, riggers have their own bag of tricks. The following rules expand on the options presented in *SR4A* and other *Shadowrun* products on rigging, with an eye to answering lingering questions on cyberware, jamming, biodrones, and cyborgs.

### Jacking Biodrones and Cyborgs

A biodrone's control 'ware (see *Biodrone Control 'Ware*, p. 152, *Augmentation*) has a Device rating (see *Device Rating*, p. 222, *SR4A*) that serves as its firewall, but players may wonder if the lack of a Pilot program (except for biodrones including a stirrup interface) makes them easier to hack or spoof. The answer: yes it does. A biodrone only rolls its Device rating when resisting spoofed commands or hacking.

Cyborgs may also be jacked, but in this case the rigger is setting their skills against a skilled hacker. The obvious point of entry is the cyborg's integral commlink—perfect for sending spoofed commands or to hack the cyborg's drone body wirelessly, which you can be damn sure the cyborg is going to resist, probably through cybercombat (see *Hacking*, p. 161, *Augmentation*). If the cyborg feels sufficiently threatened to shut off its commlink, the rigger has no option but to get in close and physically jack in—and face the prospect of a pissed-off cyborg in meat-space.

A safer bet is to try and jack a cyborg body during its maintenance downtime. For the brief period when the cranial containment unit isn't attached to it, the drone body can be jacked as normal (treat it as a regular drone with a Pilot of 0), though most require the rigger to physically jack in to the drone body.

### Jamming on the Fly

More than almost any other character, riggers are dependent on wireless signals in order to use their specialty, which means that few riggers are strangers to electronic warfare. Sometimes you need to shut down another rigger or hacker and don't have a jammer available; in such circumstances you do the best that you can with whatever radio or wireless transmitter you have on hand, spitting static into whatever channels or bands the opposition is using. Jamming on the fly tends to be a noisy and difficult affair, but it can work—and that's the important thing.

Jamming on the fly is a Complex Action and requires some device with a Signal rating (such as a commlink, radio, or drone) to act as an impromptu jammer. Make an Opposed Test between the rigger's Electronic Warfare skill + Signal rating and the target's Electronic Warfare + Signal rating; the target adds the rating of any ECCM program she has running to her dice pool for the test. If the Opposed Test is successful, the signal is jammed; otherwise it is unaffected. Jamming on the fly is area jamming and affects a spherical area—the impromptu jammer's Signal rating is reduced by 1 for every five meters from the centre.

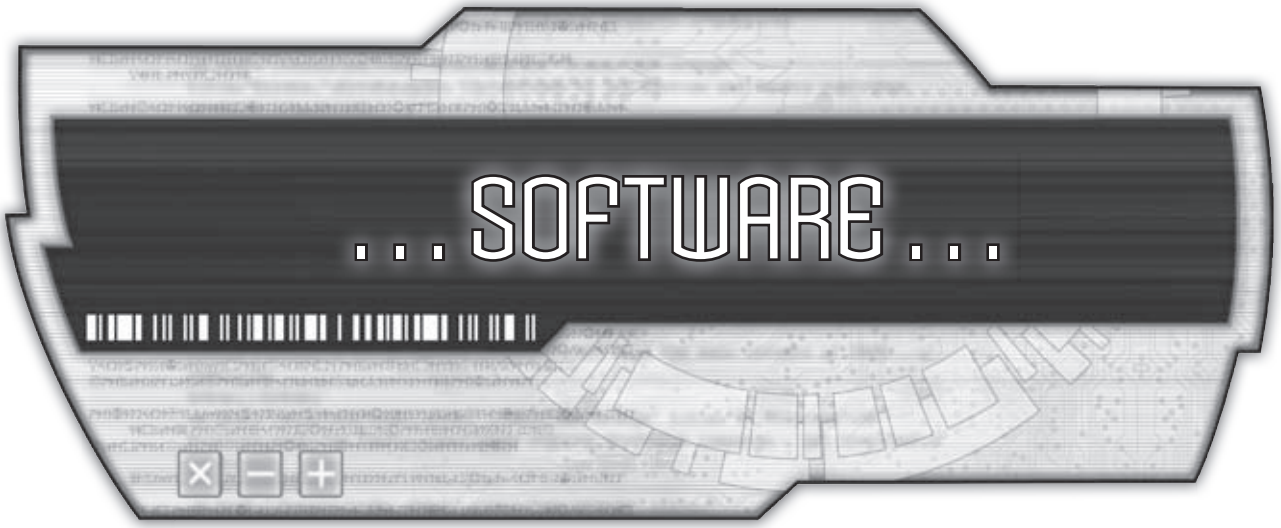
A device being used as an impromptu jammer cannot use its wireless capability for anything else. A commlink, for example, could not connect to the Matrix at the same time it is being used as an impromptu jammer.

## EMP

An electromagnetic pulse (EMP) is detrimental, if not destructive, to the operation of electronics. An EMP erases standard RFID tags but not optical-based storage media like datachips. Any non-optical and non-hardened electronic circuits within the area of effect will also be disrupted or damaged. Most "electronics" in 2070 are optical-based, but interfaces, power systems, and the like may still be vulnerable, especially on archaic systems. Affected systems may suffer data loss, power outages, or burn out entirely at the gamemaster's discretion. Wireless reception and radio communication will also be disrupted for a brief instant, which affects any wireless-only nodes, commlinks, and technomancers in the area.

EMPs have a rating that determines their intensity and area of effect. To determine the damage to a specific device, make an Opposed Test between the EMP's rating and the Device rating (see *Device Rating*, p. 222, *SR4A*) of the vulnerable electronic device. If a character is aiming the EMP at a specific device, add the character's Electronic Warfare skill to the EMP's rating when making the Opposed Test. Use the number of hits garnered to gauge the damage done to the device. Compare the EMP's rating to the Signal Rating Table on p. 222 of *SR4A* to determine the area of effect. Flying drones and vehicles affected by an EMP may also crash (see *Crashing*, p. 170, *SR4A*).

The moment of wireless disruption is not sufficient to drop an icon from the Matrix; it lasts less than a second in real-time. However, the affected icons cannot act (or be affected) during the Combat Turn that the pulse hits. Many older cyberware implants and vehicles are vulnerable to EMPs and should test for damage. Individuals and devices within a Faraday cage (a metal box or wire mesh that completely surrounds the character or device) are completely protected from an electromagnetic pulse; a cyborg's CCU is thus completely protected, but the drone body it drives may not be. If an individual or device is in a volume surrounded by wireless-inhibiting paint or wallpaper, add dice equal to their rating to the Device rating on the Opposed Test.




"We don't have time for this crap!" Medusa barked over the team's channel.

"Cool down, snakes, this firewall I'm scanning ain't no sponge," Slamm-0! snapped back. "Unlike that technowanker you used to employ, I don't just improvise code out of my virtual ass. So slap on a patch and take a deep breath, I'll be back before your buzz wears off." Remaining in the outer node of the Aztechnology gene farm he had just hacked, he opened a new connection to an address he'd received just an hour ago via digital word-of-mouth.

He toggled his VR perception to the new node, dropping into a sculpted warehouse lined with endless non-descriptive wooden shelves, each packed full of millions of items of obscure, useless kitsch. "I don't have time for this."

"Over here, boss!" the baseball browser program yelled, highlighting a small plastic dinosaur in a clutter of icons several dozen shelves over. Slamm-0! fed the dinosaur an encryption key and passcode, causing a small door to appear next to him. He stepped through the backdoor and into the new node.

"Welcome to Hacker House! We're online 24-7-365 to fulfill your hacking needs. All downloads are guaranteed virus free. We accept registered or certified cred, black escrow accounts, and one-time account transfer authorizations."

Slamm-0! discarded the intro menu. "Send priority PM to Netword: Need immediate expert advice. Pronto."

A small tornado made of millions of alphanumeric characters appeared, coalescing into the anagramic persona of Netword. "What's up, spitfire? Got yourself in trouble again? What do you need?"

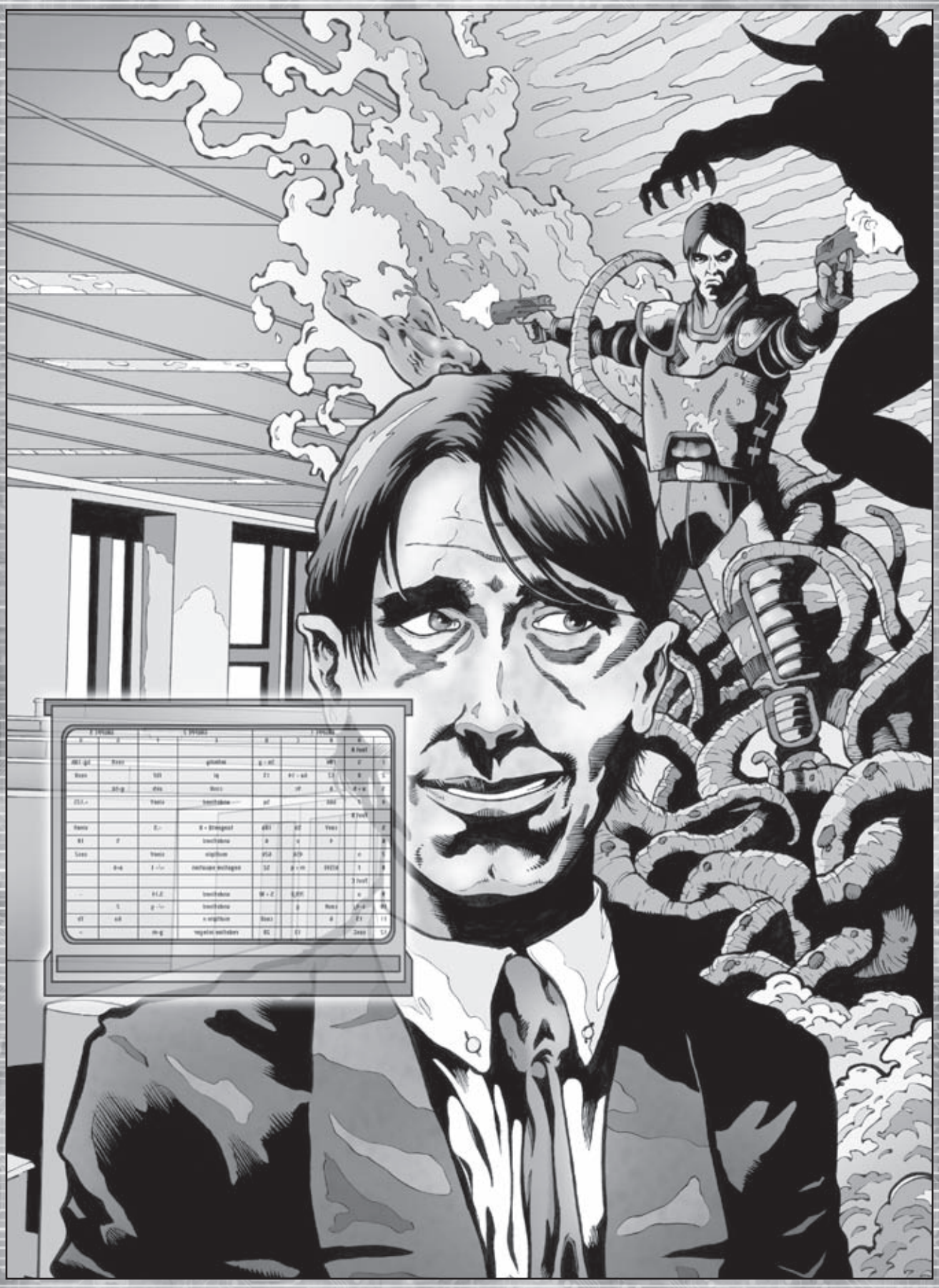
"I'm mid-run as we speak, so straight to the point: I need a cutting edge shroud to keep myself warm in an arctic node. Not that I wouldn't mind testing my new bats out on some spiders, but this time I need to pull an Artful Dodger in some Azzie system without the bells ringing. So what can you offer?"

Netword pulled up some program specs displaying a well-known dragon-head logo. "You're a lucky bastard. I just cut a deal with a German hacker who happened to get a hold of the Stealth program that S-K's eavesdropping worms use—y'know, the ones that scour the 'trix for precious info for the dragon? Anyway, it's premier code I won't offer on the boards—draws too much attention, you know? Just finished cracking the source-code and recompiling the program yesterday. You can have a copy if you're interested, but not for free. I'll accept that new Black Slugger you've been showing off in return. It would be a fine addition to my collection."

Slamm-0! hesitated. "You gotta be kidding! Do you know how many months it took me to crank out that code?"

Netword shrugged. "Take it or leave it. I'm not the one risking my life in the next few minutes."

Slamm-0! sneered, then made the swap. His new dragoncloak was already loaded when he popped back in the Azzie node and messaged his team. "I'm back, ladies. Let's hack and haul. I'm going in."



# ADVANCED SOFTWARE RULES

This section provides new rules and expanded definitions for different kinds of software and programs.

## ENVIRONMENTAL AR SOFTWARE

Due to the ability to "shape one's reality" by altering the perception of it, the augmented reality environment (ARE) software market segment has become the cash cow of many software manufacturers. The trends of the 2070s change so fast that a whole industry has developed to meet customers' ARE needs. Cool hunters roam the net for the latest fads, feeding their ideas to programmers and digital artists who aspire to meet the high demands for ARE software realism, adaptability, and exchangeability. Mass media marketing managers and advertisers promote the finished product as essential for every person's individual never-never land and distinctive social style.

Many users become so attached to there ARE-modified personal realities that they suffer cognitive lapses and social dissociation syndromes (see the Reality Impaired negative quality, p. 38). Nevertheless, the boundless possibilities of reality-shaping software in day-life has made ARE so extremely popular that many users cannot imagine living without it anymore.

The following programs are supplemental to the ARE examples given on p. 331, *SR4A*.

### Body Shop

Body Shop software incorporates a wide range of ARE fashion, from clothing and accessories to skin, hair, or eye color. Most software is designed to accentuate and complement your physical clothing and style. Don't have the cash for the latest Evo Worldware nanofaxed haute couture or Spin Shop body mods? Body Shop virtual couture is a cheap way to clothe oneself with the latest styles and mods, guaranteed to draw attention from anyone using AR. Body Shop designs are not bound by the laws of physics, of course, so it is possible to tout makeup, clothing, and hairstyles that wouldn't be possible in reality. Body Shop software varies in price depending on the features and can range from off-the-shelf outfits to designer labels or even unique, customized makeovers. Many Body Shop software houses also offer subscription services that regular update your ARE software with a new library of fresh designs, so you can keep up with the fashionistas.

### Glyphs

Glyphs are specific software "items" or artwork. Ordinary glyphs include objects that you are unlikely to find available in other AE software packages—for example, an arsenal of virtual weaponry, a pack of virtual flying scissors that follow you around, or your own personal virtual solar system of orbiting worlds and moons. Glyphs are often sold as add-ons for other ARE programs, such as a designer leash for your Virtual Pet or a Picasso for your Wall Space software. A growing industry offers specially designed glyph art pieces, often customized to the user's desire or offered in collectable limited amounts, typically carrying a watermark signature from the designing artist.

| ARE Software | Availability | Cost |
|---|---|---|
| Body Shop | — | 50-500¥ + 10-100¥/month |
| Glyphs | — | 20-5,000¥ |
| Negator | 4 | 100¥ |
| Ractives | 4 | 1,000¥ + 200¥/month |
| Scentsation | — | 50¥ |

### Negator

Negator software seeks to "edit out" anything the user programs in as "undesirable." Perfect for eccentrics, people suffering from certain phobias, or snobs who don't like to be bothered by the little people, Negator software will hide, mask, or blot out with other AR sensory input whatever they wanted negated.

### Ractives

Ractives is a common used abbreviation for "interactives." In general, these are programmed shells of virtual persona or pets that can are actually controlled by simsense-boosted actors (so-called "ractors") that play them in a subscription-based manner. Although the software is not sophisticated enough yet to actually "jump into" the shell, the instant exchange of environmental and social data between the "host" and the ractive allows a new level of realism that goes beyond the programming of ordinary virtual pets and virtual persons, which have a limited array of responses and behavioral patters.

### Scentsation

Ever wished that everywhere you went smelled like roses? Scentsation software will bring that dream to life. A library of pleasant, comforting, and subtle smells will bring joy to anyone with an AR interface capable of processing olfactory data. Less reputable software houses have been known to sell scentsation software that caters to more unusual tastes and fetishes, from certain food aromas to animal smells to undergarment odors.

## LEGAL VS. PIRATED SOFTWARE

Software purchased by normal, commercial means from software vendors or online market places is considered legal software. Although the purchase of software usually does not require verification by the buyer, the actual installation of the program requires the acceptance of license agreements, registration, and activation of software components by the manufacturer's Matrix site that involves SIN validation and authenticity cross-referencing. Due to the threat of piracy and illegal filesharing, SIN-based software registry is a universal security feature.

In game-terms, legal registered software is equipped with both the Copy Protection and the Registration program options (see p. 115). Note that all Common programs (Analyze, Browse, Command, Edit, Encrypt, Purge, Reality Filter, and Scan), agents, autosofts, skillsofts, and commercial operating systems acquired by the basic software rules and prices (see p. 232 and 330, *SR4A*) are considered legal software that include these options by default. If bought during the game with a commlink that is linked to a forged ID, gamemasters may call for an ID check (p. 267, *SR4A*) with a verification system rating of 2–4.

Legal restricted software (mostly Armor, Biofeedback Filter, Attack, Data Bomb, Decrypt, Defuse, ECCM, Medic, Nuke, Sniffer, Spoof, Stealth, and Track) that is used by spiders and Matrix security specialists in addition to hackers is usually sold via special online vendors. The same is true for paramilitary autosofts and skillsofts that involve the use of firearms or heavy weaponry. In addition to the normal ID check, users must produce a legal license. The gamemaster

## SERVER-SIDE PROGRAMS

Server-side programs are programs loaded and run from a node, network, or nexus, which can be used at the same time by a large number of people that have the account privileges to do so. Any user who is, for instance, accessing a public library nexus is able to run the nexus's server-side browse routine to do data searches, while most accounts in an office environment have access to common programs such as Browse, Edit, and possibly Command.

Common use programs that are vital for node or nexus security (like Analyze or Purge) are often limited to security or admin accounts, to prevent hackers from meddling with them from an easily-hacked basic account. Hacking or security software is similarly restricted.

In game terms, a user with the appropriate account privileges can use these programs without running their own. In this case, the software does not count towards the user's processor limit (see p. 48), but it does count towards the node's processor limit. If these programs are used in any illegal attempt, it leaves the same datatrail as if the hacker was using legal registered software.

While each application of a server-side program can be crashed individually, hackers can also crash the whole nexus-installed suite with a Hacking + Attack (Firewall + System, 1 minute) Extended Test, though this usually raises suspicions when programs start to malfunction systemically.

may call on an additional verification test for the license if the character wants to acquire the software legally using a fake license.

The advantage of legal software is that it is regularly updated and patched. These patches include security features (regular exploit fixes and patches), anti-virus and adware protection (virus and spam library updates), and any other enhancements (updates, new versions, AR interface and iconography improvements) that bring them up-to-date with the current state of programming and security.

In game terms. legal software does not degrade in the way as pirated software (see p. 109), but leaves a datatrail when used illegally for hacking (see *Registration,* p. 115).

### Pirated Software

Pirated software—i.e. programs whose copy-protection and activation/validation anti-piracy mechanisms have been bypassed through cracking—are usually distributed by warez sites (see *Piracy,* p. 94). While pirated programs have the advantage of not being linked to a registered SIN, they are not automatically updated and patched in the same manner as legal software. Without registration and the confirmation that the copy is legitimate and licensed, the software is not authorized to connect to the manufacturer's update sites.

In game terms, illegal and pirated software—and also programs that a character has coded himself (p. 118)—degrade over time, reflecting that the program is slowly becoming outdated. Hacking and malware programs degrade at the rate of 1 rating point per month; all other programs degrade 1 rating point per 2 months.

## WAREZ DEGRADATION

By default *Unwired* assumes that all forms of cracked software, from agents to autosofts, degrade as described under Pirated Software. Groups, however, are free to adjust what programs are affected by degradation to suit their games and play styles. To reduce book keeping gamemasters may wish to limit degradation to cracked Hacking and Common Use programs, Firewalls, and autonomous constructs (ie. Pilots, IC and agents.) While the remaining types of cracked software would still suffer degradation and enforced obsolescence, the rates at which they degrade would be slower and their effects less obvious.

### GETTING HOOKED UP

To circumvent or prevent degradation of their utilities, hackers have several options available to them.

First, skilled hackers with programming resources can patch programs (see *Patching,* p. 118) on their own. Programming suites (p. 118) and nexi running programming environments (p.118) are particularly useful tools.

Second, those that have connections to warez sites can go looking for an updated pirated copy to buy (see *Finding Pirate Networks,* p. 94), or join and trade with one of the many groups of the Cracker Underground (in the form of virtual contacts see p. 129, *Runner's Companion.*) Such groups even allow hackers to trade patches they wrote for patches they need (typically for software with equal ratings though not necessarily, as supply and demand varies)—note that such groups are traditionally finicky about allowing script kiddies and autonomous agents access to their hard work and valuable warez.

Third, daredevil hackers always have the option of hacking the corporate patching nodes directly to steal the patch for themselves and their contacts.

Gamemasters wishing to reduce bookkeeping may allow hackers to update all their programs in a single go by adding the total of the patch costs to the character's monthly Lifestyle expenses—assuming the character has a dependable source such as a cracker group and makes a point of maintaining their contacts. Alternatively, at the gamemaster's discretion, all patches required can be located and bought from a warez group or cracker collective with a single Availability Test (using the highest Availability of the programs involved) and paying the sum total for all the patches.

Degradation of pirated software owes as much to systemic software and firmware upgrades demanding compatibility updates as to the megacorporations making regular updates an anti-piracy feature. In 2070, obsolescence and latent program degradation is hardcoded into software and is triggered when compromised software is flagged. Software programmed by the hacker and Open Source programs never degrade in this fashion, but may require patching to remain current at the gamemaster's discretion.

## OPTIONAL RULE:
*Freeware and Open Source Programs*

**Open Source Programs**

Though the megacorporations are actively waging a Matrix war against the open source movement, knocking it down to a fringe phenomenon, open source programs do exist. Open source software is basically computer software whose source code is readily available under a certain license that permits users to use, change, and improve the software, and to redistribute it in modified or unmodified form. It is often developed in a public, collaborative manner, though programs originating from open source are less commonly known than their corporate counterparts that are mass-marketed and heavily advertised. With the Corporate Court Matrix Authority refusing to share certain code elements of the Matrix infrastructure (hiding behind megacorporate patents for decades) with which programs are supposed to interact, corporations have effectively reduced the frequency of open source programs.

In game terms, open source programs are considered legal software that can be cheaply bought with a 50% reduction in price and which have neither the Copy Protection nor the Registration program options. Open source software degrades in the same manner as pirated software, as it tends to be updated on an irregular basis.

Alternatively, open source programs produced by warez groups might be traded for free or patched up more regularly, as long as the hacker character maintains a warez contact and contributes to the group. For each piece he contributes, the hacker may download a number of programs equal to the contact's Loyalty rating.

Gamemasters may further limit open source programs by ruling that certain program options are not available for these programs, by capping the maximum limits of these programs at a rating of 4, or by making the rating dependent on the warez contact's Connection rating.

**Freeware**

Freeware is copyrighted computer software that is made available for use free of charge for an unlimited time, though creators often retain control of the program's source code for future development.

In game terms, freeware programs carry the Copy Protection program option but not the Registration option and they can be acquired by player characters at no cost. Since freeware is coded on a non-profit basis, and the resources of single programmers or small programming groups are limited, freeware programs are limited to a maximum rating of 4. Freeware also degrades like pirated software.

Similar to open source programs, gamemasters may further limit these programs by disallowing certain program options.

### VERIFYING PROGRAMS TABLE

| Hits | Information Learned |
|---|---|
| 1 | The nature and type of the program |
| 2 | The program's rating |
| 3 | Existence of program options (+1 per additional hit) including option ratings |
| 4 | Detect code error and bugs |
| 5+ | Manufacturer or programmer (if signed) plus any further information that the program may provide |

By default only cracked Firewalls, Hacking, Common Use, and autonomous programs (ie. Pilots, IC and agents) degrade. Gamemasters may adjust what programs are affected by degradation to suit their games and play styles; a more draconic approach might include skillsofts

For more on cracked software degradation, see the *Warez Degradation* sidebar.

## VERIFYING SOFTWARE

If a character is not careful, he may purchase more than what he bargained for, especially if scoring some code from an untrustworthy black marketeer or corporate lackey. Illegally (and sometimes legally) purchased software may come with unadvertised and unwanted program options, be infested with viruses, or may be an outdated or glitchy version of the utility he asked for.

To verify that a program is what the character thinks it is or to determine what kind of program he is dealing with, he must analyze it, requiring a simple Software + Analyze Success Test. The number of hits determines how much information he gains about the program in questions, as noted on the Verifying Programs Table, p. 109.

In order to detect a virus in a program, a number of hits equal to half the virus's rating must be scored (see *Viruses,* p. 120).

## AUTONOMOUS PROGRAMS

Unlike other software, agents have the unique ability to operate independently of their controlling persona in the Matrix. This sort of autonomous operation raises several issues which are addressed here. Though we refer to agents in most cases, unless otherwise noted these rules also apply to other autonomous entities such as sprites, AIs (p. 165), and e-ghosts (p. 170).

**Node Movement and Accounts**

For an agent to operate independently of its controlling persona, it must be loaded into a node the persona has access to. The agent logs into an account like any Matrix user (either using passcodes or exploits) and has whatever privileges that account applies. The agent's software is actually running on this node (not on the persona's node any more), and so counts towards the node's processor limit (p. 48). Likewise, any other programs the agent is carrying in its payload must also be running, and so also count towards the processor limit.

Like any Matrix user, the agent can access multiple nodes at once. Other nodes must be accessed with passcodes or hacked, per normal rules. The agent remains loaded on only one node, however—though it interacts with other nodes, it does not need

to be copied and loaded on them. (In fact, legal unmodified agents are incapable of copying themselves in this manner.

The agent may *move* to another node, which constitutes loading itself onto the new node and unloading itself and logging off from the old one. Rather than moving, an agent with the Replicate autosoft and without copy protection may *copy* itself onto another node it has accessed, spawning a new version of the agent (note that sprites, AIs, and e-ghosts, as "living" digital entities, are incapable of copying themselves this way). Legal and unmodified agents are not capable of copying themselves due to copy protection (moving to another node does not count as copying because the agent is erased from the previous node as part of the moving procedure).

#### Access ID

Unlike Matrix users, agents and other autonomous programs do not access the Matrix via a device, and so they are not assigned an access ID. Instead, each autonomous program has a built-in access ID, sort of a software serial number. This ID is used when logging into nodes and interacting with other programs, and so it may be used to track the agent's activity through the Matrix, just like a hacker's datatrail.

Once running, the access ID may not be switched, not even if the agent moves and loads onto another node (as the agent must already have accessed the new node, using its access ID in the process).

#### Copied Agents and IDs

Note that when an agent program is copied, the access ID built into the agent is copied as well. This means that any copies of the agent will have the same access ID. This is not a problem when a hacker is running such copies simultaneously from his persona (as his access ID is used in that case), or if the copies are operating autonomously in independent nodes. If a copy tries to access a node on which an agent with the same access ID is already running, however, the node will automatically refuse access (even if the agent tries to hack his way in, the attempt will automatically fail). This security feature both deters piracy and prevents mass invasions by agent mooks (the so-called "Agent Smith" scenario).

A copied agent may be patched in order to give it a separate unique access ID with a Logic + Software (Rating x 3, 1 week) Extended Test.

### AGENT COMPETENCY

Agents may be capable of operating independently, but this does not mean that they are just as capable as hacker characters. In fact, while they are very smart in many ways, agents possess a number of drawbacks that make them inferior to metahumans.

The Pilot program that guides an autonomous agent is an incredibly sophisticated software with logical and analytic capabilities on par with any metahuman. This does not mean, however, that the agent has decision-making capabilities equal to metahuman. Not only do they lack a lifetime of experience to base their judgements on, they often lack the *context* that would enable them to fully understanding a situation. For example, while the agent may understand that certain icons engaged in cybercombat with others are considered enemies, and might even grasp some of the finer tactical points, it would not necessarily understand the personal relationships or social cues between them, and so would not realize that, say, attacking one icon might enrage another, or recognize that one icon is attempting to surrender or switch sides, or comprehend that one icon is simply toying with its opposition and hasn't unleashed the big guns yet. Contextual information is even more lacking when the agent interacts with the physical world in some way (via sensor, security system, or drone, for example), as agent Pilots are programmed for Matrix activities, not for interfacing with meatspace. (This is less true of drone Pilots, which are programmed for real-world activity, but are specifically tailored for the drone model they occupy; see *Pilot Capabilities,* p. 103, *Arsenal.*)

Pilots are also limited in their capacity for creative thought. They tend to stick to their orders, making strictly logical choices according to programmed decision trees (see *Agent Scripting,* p. 100)—which may not always be the best course of action. When faced with an unexpected obstacle or set of choices that don't fit their programming, they tend to fall back and regroup—a safer choice over improvisation. Note that agents due have "fuzzy logic" routines that allow them to judge and act on imprecise concepts and conditions, but taking action based on generalized probabilities also has its drawbacks.

When in doubt, gamemasters can secretly roll a Pilot + Response Test against an appropriate difficulty threshold to determine how agents respond to difficult situations based on their orders (see *Issue Command,* p. 229, *SR4A*).

## NEW PROGRAMS AND ACTIONS

This section introduces a number of new utilities and describes the use of these programs in *SR4A*.

### NEW SOFTWARE

Programs are the lifeblood of hackers and are often quite useful to non-hackers as well.

#### Corrupt (Hacking)

A mixture of Edit and Browse subroutines, Corrupt programs are designed to track down and demolish specific information in a node without actually deleting the files in which they are saved (see the *Corrupt Data* action, p. 112). The idea is that, since deleted files can be restored from back-ups, Corrupt edits the files to overwrite the targeted information while leaving the file intact, without making any indication of the alteration, so that the corrupted file is eventually backed up as well, making detection and recovery of the original more difficult.

Additionally, Corrupt programs can be attached to a particular file in the same manner as *Data Bombs* (p. 233, *SR4A*). If triggered, the Corrupt program demolishes the data before it can be accessed. Corrupt programs used in this way can be deactivated in same manner a Data Bomb is defused (see *Disarm Data Bomb,* p. 230, *SR4A*).

### Disarm (Hacking)

Disarm is used to undermine programs without crashing them. It is used to corrupt targeted software so that the disarmed program cannot act against the hacker (and only the hacker), effectively neutralizing its use. Operating systems, personas, IC, agents, sprites, and malware may not be disarmed, but this utility is effective against most Common Use programs, Hacking programs, and autosofts.

### Nuke (Hacking)

Nuke is a combat utility that does not inflict Matrix damage, but instead hogs up system resources in an attempt to freeze the target user. Treat damage from a Nuke attack similar to Matrix damage from an Attack program. However, each box of Nuke damage instead deducts one point from either the node's Response or System/Pilot (in case of agents or sprites) with the appropriate effects on Matrix Initiative, processor limit, and subscription limits. The attacker determines which attribute is affected by each point of Nuke damage. If Nuke reduces both values to zero, the target's persona freezes. The user or agent can take no action within the Matrix until he reboots (p. 231, *SR4A*). Likewise, Response reduced by a Nuke attack cannot be restored without a reboot.

Due to the unique and organic nature of the living persona, technomancers are immune to Nuke attacks, while sprites and other autonomous entities that depend on the resources of the node they are on (rather than the technomancer), are not.

### Purge (Common Use)

The sole purpose of Purge programs is to search through nodes infected with virus programs to find the virulent code and eradicate it with a Disinfect Test (see p. 112). Purging software in this manner restores the program completely to its normal use and present rating.

## NEW MATRIX ACTIONS

Matrix actions are sets of commands or instructions a Matrix user issues to a node via a certain program to perform a specific task. Note that a character logged onto a node using an account with certain account privileges (see p. 225, *SR4A*) may automatically succeed at specific system operations, according to the limits of their account. The following system actions follow the same guidelines and rules as described in *Shadowrun, Twentieth Anniversary Edition*.

### Corrupt Data

The Corrupt Data action unleashes a Corrupt program on a particular node or device. Similar to Browse, the program is set to seek out and destroy a particular piece of information with an Extended Hacking + Corrupt Test with an interval of 1 Combat Turn. The gamemaster sets the threshold based on the complexity of the data, the size of the node, and the abundance of the data, as suggested on the Corruption Table (p. 112). The gamemaster may also modify the dice pool or threshold to account for addition factors, like encryption and protection of data.

The OS or the integrity of a node cannot be comprised by the use of the Corrupt program.

### Disarm Program

To disarm a program, the hacker must make a Hacking + Disarm (Firewall + System, 1 Initiative Pass) Extended Test. When the threshold is reached, the targeted software can no longer be used against the hacker (i.e., Analyze will not detect the hacker, Attack will not target the hacker, and so on). The disarmed software still functions normally against others. Likewise, the hacker is still vulnerable to similar software wielded by others. Disarmed software will remain neutralized until it has been reloaded or until the hacker logs off the node.

Firewalls may also be disarmed, but they feature coded countermeasures that make such attempts likely to trigger an alert. The node makes an Analyze + Firewall (Stealth) Extended Test each time a Disarm Test is made. If it meets its threshold before the Disarm Extended Test succeeds, an alert is

### THE CUTTING EDGE: *Military Grade Software*

Although normal programs are only commercially available to a maximum rating of 6, cutting edge software with a rating of 7 or higher does exist. So-called military-grade or prototype software is usually used and distributed only among governmental and military spiders, special unit hackers (like GOD or ARM agents), or the operatives of the megacorporations that develop these programs.

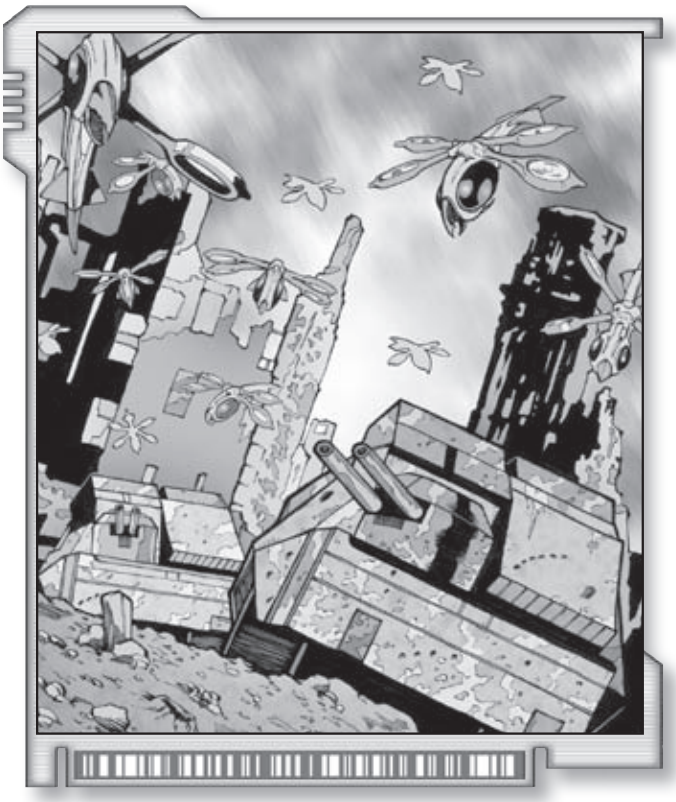
To prevent military programs from leaking into the shadows and black markets, copies of these programs are closely monitored. Use or loading of these programs is often restricted by biometric identification or the use of Limitation or Timer program options.

It is rumored that some agencies and corporations purposely infect these programs with special viruses that leave dormancy as soon as the software is transferred to a different commlink or computer system in order to wreak havoc on those systems, delete the software, and/or report its location to its originators.

The gamemaster designs exactly when and where to include such potent programs in his campaign. They should be rare at best, and finding, stealing, or otherwise acquiring such software could be an adventure unto itself—not to mention keeping it.

### CORRUPTION TABLE

| Threshold | Corrupted Data Task |
|---|---|
| 2 | Corrupt some specific information on a basic commlink |
| 4 | Compromise a criminal dossier in a police database |
| 8 | Impair all copies of a file in a corporate nexus |
| 15 | Corrupt every mention of Aztechnology's secretive board of directors from Jackpoint |
| 20+ | Scramble all SINs with the same biometric data in the Global SIN Registry nexus |



triggered, and the Firewall immediately reconfigures itself so that the Disarm attempt must be restarted.

Note that Disarm may not be used against Data Bombs—Defuse is required for that.

### Disinfect

In order to disinfect a virus, you must first have detected the virus (see *Viruses,* p. 120). Once detected, the virus can be purged with a Complex Action and an Opposed Test pitting Computer + Purge vs. the Virus Rating x 2. If successful, the virus and all copies of it residing in different programs in that node are removed.

If a node is infected by more than one virus, a test must be made for each separate virus (this is considered part of the same Complex Action, however).

## NEW AUTOSOFTS

Autosofts are specialized programs that expand the options and capabilities of Pilot programs. Autosofts provide a specific skill or new ability that goes beyond the normal programming of either the drone's dog brain or an agent's frame programming.

### AGENT AUTOSOFTS

Agent autosofts are expert programs designed to augment Matrix agents and IC; they are not compatible with drone Pilots. Programmed mainly by Matrix security companies (because of the complexity of an autosoft's programming), these subroutines are adaptive add-ons designed to put IC on par with intruding hackers or malware agents (like worms). To match the opposition, however, hackers also integrate autosofts into their agents and worms.

Agent autosofts follow the same rules for cost and programming as drone autosofts.

#### Adaptability (Rating 1–3)

This autosoft expands the agent's capabilities for fuzzy logic and deductive reasoning, factoring in more efficient decision-making algorithms. This adds additional dice equal to the rating for comprehending orders and making autonomous decisions (see *Agent Competency,* p. 111, and *Issue Command,* p. 229, *SR4A*).

#### Cascading (Rating 1–3)

Agents with the cascading autosoft are able to analyze a target's defenses, pinpoint weaknesses, and improve its attacks to better exploit those vulnerabilities. When a cascading agent misses a target in cybercombat or fails to damage a target when it scores a hit, the cascading smartsoft analyzes the defenses and optimizes its attack parameters. As a result, after each failed attack, the agent's attack dice pool increases by a number of dice equal to the Cascading rating. This increase is cumulative—each time the agents misses or the target neutralizes an attack, the dice pool is increased again. The maximum number of dice gained in this manner cannot exceed the node's Response x 2.

The dice pool bonus gained by Cascading is cleared as soon as cybercombat ends or the combatant leaves the node.

#### Expert Defense (Rating 1–3)

An agent programmed with the Expert Defense option is quite good at defending itself. Each point of Expert Defense adds an additional die to defense rolls made by the agent, up to a maximum bonus of 3. Expert Defense is incompatible with Expert Offense.

#### Expert Offense (Rating 1–3)

Agents programmed with the Expert Offense option make more effective attacks. Each point of Expert Offense adds an additional die to Matrix Attack Tests, to a maximum bonus of 3. Expert Offense is incompatible with Expert Defense.

### AUTOSOFTS AND DAILY LIFE

The ubiquitous use of drones has lead to the development of a plethora of different and often very specialized autosofts for drones equipped with the proper mechanical tools to actually execute the task governed by the software. The most common autosoft suites are designed for housekeeping tasks such as cooking, cleaning, groundskeeping, and home maintenance, allowing drones to skillfully complete household chores without constant supervision. Other mainstream autosoft packages include traffic management, construction, firefighting, pest removal, and farming/crop maintenance.

One interesting new type of autosofts helps a drone to respond more effectively to human behavioral patterns based on the input the drone receives from sensor software (particularly Empathy software, p. 60, *Arsenal*). Many drones have benefited from this new advance in autosoft programming, including creature-like pet drones that respond to their owner' emotional states with realistic animal patterns, robo-nannies that take care of an infant's needs, and, of course, anthroform sex bots.

### Homeground (Rating)

Agents that carry the Homeground autosoft are optimized to function in a specific node on which they are run. Attuned to the node's particular characteristics, they will spot any anomalies or peculiarities like a breach of security more easily. Apply a dice pool modifier equal to the Homeground rating for all Matrix Perception Tests undertaken in their home node.

### Replicate (Rating)

Replicate is a malware autosoft usually integrated into worms so that they can multiply themselves and spawn to other devices and nodes (see *Node Movement and Accounts* p. 110). In game terms, a worm-like agent equipped with this autosoft draws on the system's resources to reproduce itself onto another node to which it has access, including all the programs it has loaded, as long as these can be copied (i.e. they don't carry the Copy Protection program option, p. 114). The worm makes a Pilot + Replicate (Pilot x 4, 1 Combat Turn) Extended Test to determine how long replication takes.

## DRONE AUTOSOFTS

With the integration of drones in different areas of operations like security, factories, households, or even war zones, the demand for adaptability and modular enhancement of general drone designs to specialized tasks is high. Autosofts, which can be easily loaded and unloaded from a drone, allow the expansion of drone abilities when not controlled by a rigger, providing them with greater autonomy and functionality.

### Adaptability (1–3)

Same as the agent autosoft on p. 113.

### Chaser

This program enables the drone to shadow someone without being noticed, using sensor-based targeting and evasion patterns. The drone will also analyze mapsofts and other information to predict possible routes the targeted individual is likely to take. The drone rolls Chaser + Pilot while following someone (Shadowing Tests).

### Covert Ops

This program enables the drone to adapt to the present environment to evade detection, go unnoticed, or actively sneak past guards. A drone equipped with a Covert Ops autosoft can make Infiltration Tests using Covert Ops + Pilot to avoid being spotted or pass electronic sensors.

### [Profession]

Profession autosofts are the equivalent of a single Technical or Knowledge skill. It allows a drone with the proper equipment and specs (tools or working arms) to perform the task, rolling Pilot + [Profession] for the test. What skills are available as [Profession] autosofts are up to individual gamemasters, but as a rule of thumb Technical and Knowledge skills that require creative ability and sophisticated decision-making like Artisan, Hacking and Software should not be available.

### Trailblazer

This autosoft is often employed by border patrol drones. It provides the drone with the necessary information to pursue and track down metahuman targets in the wilderness by detecting and following trails and calculating paths based on probability functions, environmental sensor scans, and mapsofts. In game terms, it enables the drone to make Tracking Tests rolling Trailblazer + Pilot.

# PROGRAM OPTIONS

Program options are modifications to a program that alter its basic operation. In the 70s, computer programs feature modular designs that allow their functions to be easily enhanced (or limited) by add-ons, subroutine plug-ins, or patches. Options, however, dramatically increase the complexity of the software rules. The interaction of options and programs can become quite intricate, so gamemasters and players should become thoroughly familiar with the standard rules before introducing options into their games. Gamemasters may, of course, choose to only introduce specific options into their games.

Only Common Use (p. 232, *SR4A*), Hacking (p. 233, *SR4A*), Autosoft (p. 246, *SR4A,* and p. 112), and Simsense programs (including BTLs and skillsofts) may be equipped with program options.

Each program can be maximally equipped with a number of options equal to half its rating (round down). If a program does not possess a rating (like BTLs), it can carry only 1 program option unless the gamemaster decides otherwise. Note that Copy Protection and Registration do not count towards this limit. Technomancers can implement program options into complex forms as described on p. 136 and p. 148.

Some program options have a rating; unless otherwise noted, the range for this rating is 1–6.

## GENERAL PROGRAM OPTIONS

These options are available to several different program types, as individually noted.

### Biofeedback (Rating Stun or Physical)

**Program Types:** Hacking (Data Bomb only), Simsense

Programs can be equipped with a Black IC biofeedback subprogram that inflicts damage on a user. This option is commonly used for both Black IC Data Bombs (so called Black Pits) and Black Death or Black Night chips (BTL programs designed to kill or torture a user). In game terms, these programs inflict either (rating) Stun or Physical damage directly to the user every time the subroutine is triggered by the program, resisted with Willpower + Biofeedback Filter. In case of Data Bombs, this damage is in addition to the normal Matrix damage inflicted by the bomb itself.

### Copy Protection (Rating)

**Program Types:** Common, Hacking, Autosoft, Simsense

Copy Protection prohibits the program from being copied (see *Legal vs. Pirated Software,* p. 108).

### Crashguard

**Program Types:** Common, Hacking, Autosoft, Simsense

Programs with the Crashguard option are harder to crash. Add six dice to a Firewall + System roll to resist a Crash Program attempt (see p. 230, *SR4A*).

### Ergonomic

**Program Types:** Common, Hacking

Programs equipped with the Ergonomic option do not count towards a node's processor limit (see p. 48) or an agent's payload

(p. 234, *SR4A*). Note, however, that there is a limit on how many ergonomic programs you can have loaded equal to the processor limit or payload.

### Limitation

**Program Types:** Common, Hacking, Autosoft, Simsense

A program with the Limitation option has some sort of restriction parameter that prohibits the software from being used in certain ways and under specific circumstances (for instance when a pre-determined trigger situation is met).

**Common/Hacking:** The Limitation option restricts the program to a single type of target, such as personas, agents, sprites, or AIs (it is useless against any other type of target) or prohibits its use against a persona/agent/sprite/AI carrying a certain passkey code. Some corps are known to include the latter variant of the Limitation option on attack programs they sell so that the programs cannot be used against their own spiders or IC. In addition, programs that are released as shareware typically feature a Limitation option that prohibits the use of parts of the programs or prevents it from being run above a certain rating until the software has been purchased and registered.

**Simsense:** The Limitation option manifests as a mental block that prohibits the use of a skillsoft against certain targets (a Lone-Star cop, corporate grunts carrying a certain logo) or restricts the use of a combat skill to certain brands of weapons. Mental block Limitations can be tied to any particular trigger condition the user is able to experience.

**Autosoft:** The Limitation imposes a restriction on what drone brands the autosoft program can be used or prohibits the use against certain targets it has identified by sensor or which carry a certain electronic signature that the drone can recognize.

### Mute

**Program Types:** Common, Hacking

The Mute option is intentionally designed to confound and confuse node alarm systems. If a program with the Mute option is used in an action which triggers an alarm, the alarm is temporarily delayed for one full Combat Turn.

### Optimization (Rating)

**Program Types:** Common, Hacking, Autosoft, Simsense

Under normal circumstances, a node's System rating limits the rating on any software run on that node (see *System,* p. 222, *SR4A*). A program with the Optimization option is more effective at running on a system with limited resources. Add the Optimization rating to the rating of the System (to a maximum of twice the System's rating) to determine the maximum rating at which the program can operate.

### Psychotropic (Rating)

**Program Types:** Black IC-capable combat programs or Simsense

Psychotropic software uses brute-force simsense biofeedback to imprint a victim with a certain lasting psychological effect. Each Psychotropic program inflicts a specific effect in the form of a Negative quality. In consequence, the victim's subconscious is "programmed" with subliminal messages without his knowledge.

The Psychotropic program option can only be added to a program that features some kind of biofeedback subroutine (for example, a Black IC program like Black Hammer or a program with the Biofeedback program option).

Psychotropic-modified attacks function in the same manner as normal Black IC attacks (p. 237, *SR4A*), with the following addition: each time a character takes damage from a Psychotropic Black IC attack, the user must engage the program in an Opposed Test pitting Willpower + Biofeedback Filter vs. Black IC rating + Psychotropic rating. If the Psychotropic program scores more hits, the subroutine implants its psychotropic effect in the character's mind. See the Psychotropic-Induced Qualities sidebar for suggestions on appropriate qualities.

Note that a character afflicted with a psychotropic effect will not be consciously aware of it. When he first experiences the effect, his initial response will be to rationalize his behavior. Others must

#### PSYCHOTROPIC-INFLICTED QUALITIES

Because psychotropic conditioning has a limited period of time to imprint a victim's brain, only the crudest form of psycho-emotional effects may be applied. Finer brainwashing techniques require time, expertise, and a more sophisticated regimen of simsense and drugs (see *Programmable ASIST Biofeedback,* p. 189). Instead, psychotropic IC uses basic cerebral imprints that are effective on almost all metahumans.

The gamemaster has final say on which qualities psychotropic IC may inflict on a target. A few suggestions are provided below. Gamemasters are also encouraged to create their own, similar, qualities.

- Addiction (Mild or Moderate) p. 93, *SR4A*
- Augmentation Addict p. 21, *Augmentation*
- Chronic Disassociation Syndrome p. 163, *Augmentation*
- Codeblock p. 94, *SR4A*
- Combat Paralysis p. 94, *SR4A*
- Delusion p. 163, *Augmentation*
- Emotion Leak p. 163, *Augmentation*
- Incompetent p. 95, *SR4A*
- Mania/Phobia (up to 15 BP) p. 164, *Augmentation*
- Media Junkie (Mild or Moderate) p. 37
- Obsessive-Compulsive Disorder p. 164, *Augmentation*
- Reality Impaired p. 38
- Scorched p. 95, *SR4A*
- Simsense Vertigo p. 95, *SR4A*
- Virtual Personality p. 38

Rather than inflicting a full-blown quality, psychotropic IC could also inflict a short-term emotional adjustment lasting for (rating) hours. This may include effects such as aversions to certain things, desire for a certain product, complacency or lethargy, guilt, paranoia, phobias, and so on. These may be associated with a specific trigger, such as an aversion to the Matrix, an insatiable urge to eat Nerps, a phobia of trolls, or frothing rage at the sight of Lone Star officers. Short-term memory loss is also an option.


point out the character's unusual behavior before he can grasp the true cause of the effect. At the gamemaster's discretion, inflicted qualities may be bought off with Karma (see p. 271, *SR4A*) or erased with PAB reprogramming (see p. 196).

### Registration

**Program Types:** Common, Hacking, Autosoft, Simsense

A program that is equipped with the Registration option was bought and registered online via a valid (appearing) SIN, which is written into the registry of the program. As a consequence, the software is regularly updated by the company that sold the program and thus is immune to degradation (see *Legal vs. Pirated Software,* p. 108).

Since the software is registered, however, it leaves a datatrail that allows its usage to be more easily tracked. As a result, hackers have to be more careful about "cleaning up" behind them.

In game terms, decrease the threshold of any attempts to track a user who has used a registered program by 1 for each registered program used. Likewise, increase the threshold of any attempt to Edit the access log (p. 65) or otherwise eliminate traces of the datatrail by 1 for every registered program used while hacking a node.

### Timer

**Program Types:** Common, Hacking, Autosoft, Simsense

The timer option counts down to a specific time or records the number of times a program was used (or played in case of BTLs). As soon as the pre-chosen trigger is met, the program erases itself and all copies. Demo programs are usually equipped with this option, so that they may be tried once or for a limited period before they self-erase.

Only programs without the Registration option can have a Timer option, thus Timer programs are not updated and are subject to software degradation just like pirated software (see p. 109).

**Cracking the Timer:** The self-erasing features of the Timer option can by bypassed by a Software + Logic (10, 1 hour) Extended Test (using Hardware instead of Software in the case of programs run from a chip, like some skillsofts).

### Viral Resistance (Rating)

**Program Types:** Common, Hacking, Autosoft, Simsense

Programs carrying the Viral Resistance option are less prone to viral infection. Reduce the virus's dice pool by a number of dice equal to the Viral Resistance rating for Infection Tests made by the virus or for hackers who install them directly (p. 121).

## HACKING PROGRAM OPTIONS

These options may only be applied to hacking programs.

### Area (Rating)

**Program Types:** Hacking (Combat programs only)

The area option enables a combat program to engage multiple targets at once (the attacker chooses his targets, but all targets must be in the same node). The program may engage a number of targets equal to the Area option rating. The user makes a single Matrix Attack Test, reducing his dice pool by 1 for each additional

target beyond the first. The hits are compared to the defending icons' hits separately for each icon. In all cases where the attacker scored more hits, the attack succeeds.

#### Armor Piercing (Rating 1-3)

**Program Types:** Hacking (Combat programs only)

Any damaging program can be equipped with the Armor Piercing option, granting the program the ability to pierce software redundancy systems (Armor programs) in the same way as weapons and bullets can shoot through normal ballistic or impact armor (see *Armor Penetration,* p. 162, *SR4A*).

#### Pavlov

**Program Types:** Hacking (Data Bomb only)

Pavlov is an option specific to Data Bomb programs. A Pavlov Data Bomb does not crash when detonated and remains armed, but is in all other regards handled like a normal Data Bomb (see p. 233, *SR4A*).

#### Rust

**Program Types:** Hacking (Combat programs only)

Combat programs equipped with the Rust option are designed to degrade an Armor utility over time. For each successful attack on a target (each attack that hits, regardless of whether it causes damage), reduce the rating of its Armor program by 1. This temporary degradation can be restored by reloading the program into the persona (see p. 232, *SR4A*).

#### Shredder

**Program Types:** Hacking (Exploit programs only)

The Shredder option enables the Exploit program to more effectively subvert code that stabilizes a program or OS. Apply a +2 dice pool modifier for all Crash Tests.

#### Targeting

**Program Types:** Hacking (Combat programs only)

The Targeting option enables an offensive cybercombat program to zero in on a target and pinpoint its weaknesses, providing a +2 dice pool bonus on Matrix Attack Tests.

| Program Option Type | Availability (per option) | Cost (per option) |
|---|---|---|
| General* | +1 | +(Rating x 100¥)† |
| Biofeedback | +12R | +(Rating x 500¥) |
| Psychotropic | +16R | +(Rating x 1,000¥) |
| Hacking | +2R | +(Rating x 750¥)† |
| Simsense | +2 | +(Rating x 1,000¥)† |
| Addictive | x2 | +(Rating x 1,000¥) |

* Registration and Copy Protection are included by default in all legal software (at no extra Availability/Cost).

† Options without a rating are considered Rating 3 for cost purposes.

### SIMSENSE OPTIONS

These options may only be applied to simsense programs.

#### Adaptive Scale

**Program Types:** Simsense (Skillsoft mainly)

The Adaptive Scale program option enables the user to change the rating of the program by command. It allows higher-rated skillsofts to be used on lesser skillwire systems (by running them at the lower rating). It also hands the user a certain kind of adaptability, scaling down a less important or currently not used skillsoft to free up space on a skillwire system for other skills, without swapping the programs in an out. Decreasing or increasing the rating of a skillsoft within the program's rating limits is considered a Free Action.

#### Addictive (Rating 1–2)

**Program Types:** Simsense (BTLs)

Dealers often sell special BTL programs to first-time customers that contain dangerous BTL signals that are more addictive than usual. In game terms, this option raises the threshold for Addiction Tests by its rating.

#### DIMAP

**Program Types:** Simsense (Skillsoft)

The Direct Interpretive Memory Augmentation Programming (DIMAP) option allows the user to better interpret the skillsoft's programming and more easily incorporate that information with the user's own memories. Since this brings the skillsoft skill closer to a real skill learned over time, this option *exceptionally* allows players to use Edge to reroll a failed test when using that skillsoft.

#### Lifeline

**Program Types:** Simsense (Knowsoft- and Linguasoft only)

This option for Knowsofts and Linguasofts links the skillsoft to Horizon's Lifeline online database and search engine, as long as the user of the skillsoft has some sort of active link to the Matrix. This option increases the effectiveness of the skillsoft as the software can run a very rapid, specialized data search on the connected database when the software hits something it cannot answer or translate. In game terms, the user gains a +2 dice pool modifier for each (Extended) Test undertaken with the Lifeline-equipped skillsoft as long as the user has the time (and a Matrix connection) to access the database.

Lifeline-equipped skillsoft must have a Registration program option to be functional.

#### Overdrive (Rating 1–3)

**Program Types:** Simsense (Active Soft)

Partially based on BTL technology and programming, overdrive subroutines can overclock the skillwire's firmware allowing the user to perform beyond the normal skillwire rating limits. A program with the Overdrive option adds its Overdrive rating to the dice pool rolled for tests made with the skillsoft. In effect the skillsoft runs at the "overdriven" rating and can exceed the skillwire's rating limits.

Overdriving skillwires, however, bears several side-effects:

**Distraction:** The Overdrive option makes it difficult to focus on other tasks, imposing a negative dice pool modifier equal to the Overdrive rating on all other tests performed that don't include the overdriven skillsoft. Users also often find it difficult to

deactivate the program, requiring a successful Willpower + Logic (Overdrive Rating) Test to disable the program.

**Cyberware Damage:** Overdriven activesofts can cause skillwires to break down by frying their firmware. Each time the user activates an overdriven skillsoft, make an Edge (Overdrive Rating) Test. Failure means that the overclocked soft damaged the cyberware system permanently, causing it to misinterpret neural commands or skillsoft programming. Treat any further use of the skillwire system as an automatic critical glitch. Skillwires damaged this way must be repaired with corrective maintenance or surgery (see *Installing/Repairing Cyberware or Bioware,* p. 126, *Augmentation*).

#### Personalized

**Program Types:** Simsense

The Personalized option offers greater reliability by reducing reflex action/skillwire overlay clashes. Each Personalized skillsoft must be tailored to its user's particular neuromuscular and cerebral system as well as the specifications of the individual's cyberware systems necessary to process the skillsoft. As a result, this option provides a +1 dice pool modifier for all tests undertaken with this customized skillsoft without impacting the skillsoft's rating directly. A Personalized skillsoft may not be used by someone other than the user it was personalized for.

#### Pluscode (Rating)

**Program Types:** Simsense (Activesoft)

A Pluscode activesoft reduces the demands on skillwire systems through sophisticated cache and routing algorithms, enhanced mnemonic correlation, and redundancy-integration schemes. In effect, reduce the skillsoft's rating by the Pluscode rating when applying the skillsoft towards the skillwire's maximum rating limits (see p. 342, *SR4A*). The skillsoft is still limited to a base rating equal to or less the than the skillwire's rating. The skillsoft option cannot reduce the skillsoft's impact on the rating limits to less than 1.

## SOFTWARE PROGRAMMING

To create a program from scratch—whether a new exploit tool, a home-brewed application, a patched up add-on, or a wiz piece of malware—time must be spent to crank out the code. Complex software typically involves days or even weeks of programming. Code must be constructed, debugged, rewritten, and tested before the program is finalized and ready to use. Thanks to augmented reality and the mobile Matrix, however, programmers can devote time to code-wrangling wherever they are.

### SOFTWARE CODING

The basic rules for programming are described under *Coding Your Own Programs*, p. 228, *SR4A.* All a programmer needs is Software skill and a device (a basic commlink will do) on which the program can potentially be run.

Note that due to the recording nature, format, and specialized post production techniques used to create simsense programs, neither skillsoft nor BTLs can be programmed and updated in the standard software sense. Simsense options have to be bought together with the "mother program".

| Software Coding | Avail | Cost |
|---|---|---|
| Software Programming Suite (Rating 1–5) | 6 | Rating x 1,000¥ |
| Programming Environment Access | 8 | 100¥ per day |

#### Programming Suites

A character can also enhance his programming by using a software programming suite that provide a number of useful tools such as smart editors, library packages, code optimizers, dynamic compilers, source code debuggers, and other virtual assistants. Most programming suites are designed as an augmented reality or virtual environment, allowing the character to code by manipulating menus and icons that represent basic functions, code, and features.

The rating of a programming suite acts as a positive dice pool modifier for any programming or upgrading test (but not cracking).

#### Nexus Programming

A coder can also take advantage of a virtual programming environment on a mainframe or network of connected nodes (see *Nexus,* p. 196). Programming environments are expert programming agents designed specifically for the computing capacity of corporate nexi. Unlike suites, environments do not have ratings and don't add dice to any tests for programming/upgrading. Using a programming environment, however, reduces the interval of the programming/upgrading test by half (see *Coding Software Table*, p. 228, *SR4A,* and *Advanced Programming Table*, p. 119).

While most programming environments are in the hands of corporate software developers and manufactures, independent and shadow providers do exist. The typical charge for using a programming environment is 100¥ per programming day. Naturally, mainstream hosts will require proof of identification (including SIN) and will demand certain waivers be signed; some will even require contracts or payment in advance. Some have also been known to monitor those who use their systems—either to prevent hackers from writing illegal code or to steal the code for their own purposes.

To steal programming time, a character must hack into a nexus with a programming environment and validate an account that allows them to use it. The hacker can then use the environment until the system's security notices something is wrong with the account.

#### Programming Teams

Characters may also work together in teams to produce, crack or alter programs. Programming in teams is treated as a normal Teamwork Test (p. 65, *SR4A*).

#### Coding Program Options

Coding program options is handled in the same manner as software coding. The Advanced Programming Table (p. 119) provides the thresholds and interval periods for programming these options.

If a character wishes to upgrade software he already has with new program options, he must possess the source code. Source code can be acquired by cracking the program, in the same way as circumventing copy protection (see *Piracy,* p. 94). Programs that are modified with new options are no longer considered legal programs, and suffer degradation just like other illegal software.

### Patching

As noted under *Legal vs. Pirated Software,* p. 108, illegal software does not receive regular updates from the manufacturer and so suffers from rating degradation. A hacker can still upgrade a program on his own, however, a process known as patching. In order to patch a program, the hacker must have the source code for it (acquired by cracking it, see *Piracy,* p. 94). Patching requires a regular programming Extended Test for that software type using Software + Logic and an interval of 1 week. In place of rating, however, use the difference between the degraded rating and the regular rating of the program.

## MALWARE PROGRAMMING

Like any other software, malware programs like viruses and trojans can be programmed by hackers. Instead of using the Software skill however, malware is coded using Hacking + Logic. The Advanced Programming Table (see p. 119) provides sample thresholds and interval periods for programming different types of malware programs.

Gamemaster and players should work together to create viruses and trojans that are within the capabilities of the programming character and not unbalancing within the scope of their specific game.

## SOFTWARE BUGS

A software bug is an error, flaw, mistake, failure, or fault in a computer program that prevents it from behaving as intended (e.g., producing an incorrect result). Since most bugs arise from errors in a program's source code or design, commercial vendors usually run their software through a testing phase to work out the most heinous bugs that might seriously interfere with the functionality of the program. As software companies are always under pressure to release programs on time, however, bugs often remain in early versions of released software, though these are often repaired with later updates. Likewise, due to source code theft during ongoing development, buggy (pre-)alpha and beta versions of programs often get distributed by hackers and peer-to-peer filesharers. In addition, there are a number of programmers and hackers (including player characters) that crank out their own code, selling them cheap to anyone willing (or desperate) to buy, but whom rarely have (or are willing to spend) the time to subject their programs to extensive testing.

Gamemasters may use bugs to limit or depreciate software that was bought from unreliable sources, i.e. shady dealers that want to pull a fast one. It is up to the gamemaster to decide if and when a particular program has a bug, as best suits his game. Bugs may also be discovered the hard way when a player rolls a glitch or critical glitch while using a particular piece of software.

**Finding/Repairing Bugs:** Finding and repairing a bug is handled like other programming tasks. It requires a Software + Logic (16, 1 hour) Extended Test (or Hacking + Logic in the case of malware), as noted on the Advanced Programming Table, p. 119. At the gamemaster's discretion, certain bugs may be easier or harder to find and fix, with a modified threshold as appropriate. For example, a well-known bug in a Common Use program might only have a threshold of 4, whereas a new bug in a complicated agent, autosoft, or simsense program may have a threshold of 20.

**Adding Bugs:** In certain circumstances, a character may intentionally wish to insert a bug into a program. This is handled like other programming tasks, requiring a Software + Logic (4, 1 hour) Extended Test (use Hacking if working with malware). The character must either have access to the software's source code or must crack its copy protection (see *Piracy,* p. 94). The net hits scored over the threshold (minimum 1), multiplied by 4, determine the threshold for finding and repairing the bug.

### ADVANCED PROGRAMMING TABLE

| Software | Threshold | Interval |
|---|---|---|
| Agent/IC/Pilot | Rating x 3 | 3 months |
| AR Environment | 12 | 1 month |
| Autosofts | Rating x 2 | 6 months |
| Common Use Programs | Rating | 1 month |
| Firewall | Rating x 2 | 3 months |
| Hacking Programs | Rating x 2 | 1 month |
| Sensor | Rating x 2 | 1 month |
| System | Rating x 2 | 6 months |
| Tactical | Rating x 3 | 6 months |
| **Program Options** | | |
| General | Rating* | 1 month |
| Biofeedback | Rating x 2 | 1 month |
| Psychotropic | Rating x 3 | 3 months |
| Hacking | Rating* | 1 month |
| **Malware** | | |
| Bugs (adding) | 4 | 1 hour |
| Bugs (finding/repairing) | 16† | 1 week |
| Virus | Rating x 4 | 3 months |
| Metamorphic Engine | +6 | +1 month |
| Trojan | Rating x 4 | 3 months |

* Options without a rating are considered Rating 3 for Threshold purposes.
† Subject to gamemaster discretion. If the bug is intentionally added, threshold = net hits x 4.

**OPTIONAL RULE:**
*Software Bugs & Programming*

When a character is programming software, there is the danger that bugs may be creep into the coding. Each time a character rolls a glitch while rolling the programming Extended Test, a new bug is added to the software. The gamemaster determines which specific bug is added. Note that the programmer will be unaware of these bugs until they are discovered in use.

If a critical glitch is rolled, the bug might be so fatal that the program doesn't run at all. The bug must be located and corrected for the software to function as intended.


### Bug-Ridden

**Program Types:** Common, Hacking, Autosoft, Simsense

The program is so riddled with flaws that it often crashes while in use. Make an Edge (1) Test each time the program is used. If the test fails, the software crashes. Crashed programs must be reloaded (see *Programs,* p. 232, *SR4A*).

### Deadlock

**Program Types:** Common, Hacking, Autosoft, Simsense

The program causes a fatal operation in the node, crashing the OS and causing the device to reboot. Make an Edge (1) Test each time the program is used. If the test fails, the OS seizes up and crashes.

### Defective

**Program Types:** Common, Hacking, Autosoft, Simsense

The bugs in this program seriously impede with the software's intended function. Reduce its effective rating by half (round down) to a minimum rating of 1.

### Fatal Flaw

**Program Types:** Common, Hacking, Autosoft, Simsense

This bug is a more serious version of either Bug-Ridden or Deadlock. It functions just like each of those bugs, except that after the crash, the program is fatally corrupted and cannot be reloaded. The program must be reinstalled.

### Pre-Release

**Program Types:** Common, Hacking, Autosoft, Simsense

The program is a (pre-)alpha or beta version of the real software. It runs, but with reduced effectiveness. Reduce its effective rating by 1 (to a minimum of 1).

### Quirks

**Program Types:** Simsense (Skillsoft)

Quirks are certain distinctive personality characteristics or odd habits that were copied when the skillsoft was recorded and are imprinted on the user together with the actual skill. These quirks can be anything from certain preferences for combat moves or trick actions (swirling the gun before holstering them) to speech impediments or peculiarities or nervous habits (twitching, itching). These should not be handled as a true disadvantage but can be annoying or even become a recognition feature of the character if it is prominent.

### Resource Allocation Error

**Program Types:** Common, Hacking

An advanced version of Bug-Ridden, this bug works the same except that when the program crashes, it ties up some of the node's processing power, reducing Response by 1. The program can be reloaded, but Response remains reduced until the node reboots.

### Static

**Program Types:** Simsense (Skillsoft)

Static skillsofts are defective programs that are usable but emit a distracting white noise in the user's head. Users that don't mind the noise often consider them a bargain because these programs are cheaper. In game terms, Static programs impair the user's Perception with –2 dice pool modifier while the skillsoft is actively used.

## MALWARE

Malware (short for "malicious software") is software designed to infiltrate or damage a computer system without the owner's informed consent, undermining system security. It encompasses a variety of hostile, intrusive, and annoying software or otherwise uncontrollable program code like viruses, worms, and trojans.

## VIRUSES

Viruses are self-executing proactive malware programs that infect other programs to impair them or damage the node on which these programs are run by affecting the node's operating system.

In game terms, viruses are treated as malware program options that can infect certain types of software. Each virus falls into a particular category (its so-called virus *species*) and possesses a rating that determines how sophisticated and nasty it is. While this rating usually ranges from 1 to 6, some cutting-edge viruses may rank higher at the gamemaster discretion.

### Metamorphic Engines

Like all other illegal or pirated software that is not continuously patched up by software companies, viruses are also

prone to degradation. This is in part due to the continual improvement of the virus detection abilities of programs such as Analyze or Purge. A virus's rating decreases at the rate of one point per month.

Only viruses that carry a so-called *metamorphic engine* are immune to this degradation. The metamorphic engine is a subroutine that allows the virus to adapt and update itself in order to subvert detection and removal programs. Viruses with metamorphic engines, however, are much harder to acquire or program.

### Infection of Programs

Whenever virus-ridden software is actively used in a Matrix action or test, the virus tries to infect another piece of software (gamemaster's choice) that the user has access to either on the same node or in other accessible nodes (for example, a slaved node, or another node in a cluster). The gamemaster determines what software the virus targets; some viruses target particular programs, others choose randomly. Both active and inactive programs may be infected.

Make an Opposed Test pitting the virus rating x 2 against the node's Firewall + System. If the virus succeeds, it infects the targeted software, embedding a copy of its virus code into that other program. If the node wins, it has successfully located the virus and prevented infection and will alarm the user or system administrator.

Note that infection is not only restricted to programs that "belong" to the node the virus is on (i.e., programs stored somewhere on that node). The virus may also infect programs run by a persona that is accessing the node—this is, in fact, how viruses are commonly spread. In this case, the infection test is made against the persona's node, not the node the virus is in.

### Detection and Purging of Viral Software

The detection of virus-infested software depends on how the virus passes the Firewall. If a virus-carrying program is (down) loaded on a commlink or computer system, the system makes an Opposed Test pitting its Firewall + Analyze versus the Virus rating x 2 to see if it detects the virus, applying a –4 modifier to the firewall's roll. If it succeeds, it will block the download and alarm the user or system administrator.

To detect a virus *post-infection*, the Matrix user must actively search for it (i.e. *Observe in Detail*, p. 147, *SR4A*) by performing a Matrix Perception Test (p. 228, *SR4A*). The virus opposes this test, rolling Rating x 2.

Since virus code is actually copied into the infected software, viruses cannot be attacked in cybercombat, nor will rebooting a node make a virus go away (it respawns with the infected program). Infected programs may, of course, be crashed or deleted. To remove a virus and recover the original program, however, the user must perform a Disinfect Test with an antiviral Purge program (p. 111).

### Viral Warfare

Virus-seeding hackers will often help a virus circumvent a firewall by installing the virus directly while hacking a node. Infecting a targeted program this way requires a Hacking + Edit (Virus Rating x 2, 1 Initiative Pass) Extended Test.

#### TECHNOMANCERS AND MALWARE

As complex forms and the living persona are fueled by Resonance rather than regular code, technomancers are virtually immune to malware. Viruses usually fail to recognize complex forms as a viable host and are not able to infect them. Trojans cannot enter a technomancer's living node, though technomancers can exploit trojan horses just like any hacker. Though worms will also fail to infect the living node of a technomancer, they can attack technomancers they encounter in a normal node.

Amazingly, no technomancer has managed (so far ... ) to create or shape a complex form that has the abilities of either a virus, worm, or trojan horse, though it is rumored that the creation of malware is within the capabilities of dissonant technomancers and entropic sprites (p. 179).

## SAMPLE VIRUSES

The following section describes the most annoying and dreaded viruses currently floating around in the 2070s. This is by no means an exhaustive list of the countless versions and species that have been compiled by insidious hackers, just a representative sample of the most common ones that hackers and other characters may deal with while interacting with the Matrix. Gamemasters and players are encouraged to explore these and expand upon them with their own, as necessary for their games.

### Buzz

**Infected Program Types:** Simsense (Skillsoft)

This virus contains BTL-like subroutines that are written into the target program, thereby creating a brain-bending skillsoft. For example, a moodchip-program (see *Moodchips,* p. 259, *SR4A*) may be integrated so that the user receives a sensual or invigorating sensation whenever the skillsoft is accessed. Because the user is receiving BTL effects, he could become addicted in the same way as if he used the BTL directly (see *Addiction Test*, p. 256, *SR4A*).

### Flicker

**Infected Program Types:** Common, Hacking, Autosoft

The virus opens or closes the node's wireless connections randomly, causing the node to switch between different modes (active, passive, hidden), thereby impairing it.

### Inertia

**Infected Program Types:** Common, Hacking, Simsene, Autosoft

Inertia viruses infect programs to render them functionally inert—they appear to be running, but they fail to respond as needed. Whenever a character tries to use the program, it fails to perform as desired (though the virus still tries to infect another program in the node of the same type). In game terms, the software does not provide its rating in dice to an attempted test.

### Jingle

**Infected Program Types:** Common, Hacking

A spam virus, Jingle bombards users of the node (in both AR and VR) with pop-up advertisements, spam messages, dubious offers, commercial jingles, or even politically-motivated media blitzes (anti-corporate, eco, anti-meta, anti-fascist, etc.).

### Looper

**Infected Program Types:** Simsense (Activesofts)

Skillsofts infected with the Looper virus have trouble interacting with the firmware of the character's knowsoft link or skillwires. Whenever the skillsoft is used, the character will be caught in a feedback loop and will become unable to stop using the skill forcing the user to repeat an action over and over. The effect lasts (Virus rating) hours, or until the virus is purged.

### Pacifist

**Infected Program Types:** Combat programs

This specialized variant of the Inertia virus specifically targets programs used in cybercombat. Although it appears as if they function normally, the virulent code prevents the program from actually translating damage to the target's condition monitor or in the form of lethal biofeedback.

### Slave

**Infected Program Types:** Common, Hacking,

This prankster virus blocks the user from executing certain actions or commands (accessing an icon, browsing, using a specific program, transferring cash) until he has followed an "order" from the virus (for example, reciting a certain political slogan, visiting a certain Matrix site, donating cred to a certain cause, sent a photo to certain address, etc.). Though following these orders may slow the user down, this virus is intended to annoy the user more than cause lasting damage.

### Splice

**Infected Program Types:** Common, Hacking, Autosoft

Similar to activators or deactivator (p. 116, *Augmentation*), the virus either subscribes or unsubscribes the persona to various nodes without the user's permission.

### Swiss Cheese

**Infected Program Types:** Common, Hacking, Autosoft?

This virus impairs the effectiveness of the commlink's firewall, effectively reducing its rating by 1 per copy of the virus in the node.

### Ticker

**Infected Program Types:** Common, Hacking, Autosoft

This virus is designed to try and crash a node after a pre-programmed amount of time has past. Once the timer has activated, the virus attempts to crash the OS, rolling its Virus rating x 2 in place of Hacking + Attack (see *Crash Program,* p. 230, *SR4A*).

### Unplug

**Infected Program Types:** Common, Hacking

One of the most malevolent viruses out there, Unplug is designed to reformat a node, deleting the entire OS and all programs and data within memory. Once it has infected a node, the virus makes an Virus rating x 2 (System + Firewall, 1 minute) Extended Test. As soon as the reformatting begins, the OS will alert all security and admin users, so that they may take action to eradicate the virus and cancel the reformatting.

## WORMS

Worms are reactive and autonomous malware agents used specifically to target nodes. Worms are designed to spread actively to achieve certain goals, impair or disrupt computer systems or commlink networks, delete or encrypt files, acquire and send documents, or to create zombies and botnets.

Worms are treated as independent intruding agents for rule purposes, using the Response attribute of the node on which they are currently operating (or conquering). Although a number of worms possess the ability to replicate by the means of a special agent autosoft (p. 112), not all worms require this special program to be effective malware.

### Encountering Worms

Since worms are basically agents, they cannot be disinfected or purged by antiviral software—they must instead be overcome in cybercombat. Another option is to shut down the node, which dumps the worm.

## SAMPLE WORMS

Here are a few examples of worm templates designed to perform different tasks in a node.

### Baitworms

Baitworms provoke intrusion alarms in infiltrated nodes to draw the attention of IC and spiders, allowing the hacker that deployed it to sneak past the distracted virtual opposition.

**Programs:** Armor, Attack, Exploit

**Autosoft:** Replicate

### Crashworms

Crashworms seek to undermine software integrity, causing programs to crash or suffer from induced errors. Besides crashing programs and operating systems, these worms are also sometimes used to intentionally seed bugs into software loaded onto a node. To accomplish this, the crashworm must either find a program's source code or crack it using Pilot rating (see *Piracy,* p. 94), and then insert the bug using the rules for *Adding Bugs,* p. 119. Hackers can also load a crashworm with an already buggy program, and instruct it to overwrite existing software with the buggy version.

**Programs:** Attack, Browse, Edit, Exploit, Stealth

**Autosoft:** Replicate

### Cryptoworm

Cryptoworms are designed for cryptoviral extortion attacks. Once they have infiltrated a node, they either encrypt network communications or stored files, preventing other users from accessing them. While some cryptoworms are used to force the owner into paying for the encryption keys (so-called "ransomware"), hackers also use them to temporarily blind or impede security networks and spiders during runs.

**Programs:** Browse, Edit, Encrypt, Exploit, Stealth

### Dataworms

Dataworms are a stealth tool designed to steal IDs, credit information, passcode accounts, commcode information, or passwords and transfer them to a certain site, where the deploying hacker can access them.

**Programs:** Browse, Decrypt, Edit, Exploit, Stealth
**Autosoft:** Replicate

### Deathworms

Deathworms are IC-like weapons designed to knock users offline or even stun/kill hot sim VR users.

**Programs:** Attack, Black Hammer or Black Night, Exploit, Stealth
**Autosoft:** Replicate

### Ringworms

Unlike their counterparts, ringworms are relatively benign; they are primarily used as a prankster tool. Ringworms are programmed to alter both the coding of a persona icons and AROs/VR sculpting, changing their iconography and appearance. These changes can be minor or drastic, random or according to a specified theme.

**Programs:** Edit, Exploit, Stealth

### Shutterworms

Shutterworms are a favorite of runner teams and other thieves. Shutterworms seek out any and all cameras (and sometimes other sensors) attached to the node (using Browse) and blind them (using Edit). A variant of the shutterworm attempts to crash sensor devices (using Attack in place of Edit).

**Programs:** Browse, Edit, Command, Stealth

### Tapeworms

Tapeworms erase or corrupt files that are either present or being downloaded onto a node. Often tapeworms are looking for certain keywords in files that the creator of the worms wants to be removed.

**Programs:** Browse, Corrupt, Edit, Exploit, Stealth
**Autosoft:** Replicate

### Trackerworms

Trackerworms hide inside an infiltrated node and carefully log everything the system does, periodically transmitting this log to a predetermined destination.

**Programs:** Browse, Edit, Exploit, Sniffer, Spoof, Stealth

## TROJANS

Trojans are auxiliary malware programs designed to augment hackers. Unlike viruses, which infect programs, trojans do not insert their code actively into other computer files. Instead, they present themselves as legitimate programs (like a game, virtual pet, trideo file, glyph, minor utility, or piece of ARE software) so that users unwittingly download, install, and execute these programs, thereby bringing the "trojan horse" into the system and bypassing the firewall. To prevent detection by analyzing software, the malware part of the trojan is hidden deep within the legitimate program façade. The façade program will in fact function as normal (in order to not attract attention).

### Creating Trojan Programs

Trojans are created using the standard programming rules, requiring a Hacking + Logic (Rating x 4, 3 months) Extended Test. The programming character must also have the source code for the program the trojan will be masquerading as.

#### The Set Up

The majority of trojan infections occur because the user is tricked into downloading and running a program on his commlink or another node. Trojans can be physically delivered (as a program on an optical chip that is then installed and run on a device) or loaded manually by a hacker who has already comprised a system, requiring a simple Hacking + Edit (10, 1 Initiative Pass) Extended Test.

Hacker groups (particularly those employed by criminal cartels) make extensive use of trojans, actively spreading them around the Matrix and setting snares for unknowing and careless Matrix users. At the gamemaster's discretion, characters may infect their commlinks with trojans when interacting with dubious Matrix sources or shady dealers selling cheap and pirated software.

The virulence of trojans is of a different nature than those of viruses, as they rely on the gullibility and carelessness of standard

users—or the successful implementation of social engineering—rather than flaws in a computer system's security. It is up to the gamemaster to decide if and when a character's online activities justify an infection.

### Activating Trojan Horses

As soon as the trojan's façade program is executed, the trojan malware hidden inside is activated as well. Most trojans are designed to immediately install something on the infected system (such as a backdoor or hidden proxy server), or to download and install some other sort of malware (such as a virus or worm). A few are designed to undertake some other sort of action, such as disarming the Firewall. Each trojan is designed with a different objective, and so functions differently, according to the gamemaster's discretion (see *Sample Trojans,* p. 124, for specific examples).

Because trojans are (unknowingly) activated by the duped user, they take action with the same account privileges as that user. This means that in many cases, the trojan's actions are considered legal and are not contested by the Firewall.

### Detecting and Disinfecting of Trojans

Since trojan horses take a variety of forms, there is no universal method to automatically locate and eradicate them. Trojans are particularly difficult to spot before they have been activated. They roll Rating x 2 to oppose Matrix Perception Tests once activated. If the trojan has not yet been activated, apply a –4 dice pool modifier to the Matrix Perception Test. A detected trojan can be purged with an Opposed Disinfect Test (see p. 121).

## SAMPLE TROJANS

Although a plethora of different trojans exist under different names and handles, some representative samples of trojan horse programs and their functions are described below. Gamemasters and players are encouraged to expand this list on their own and develop new trojan programs.

### Hijacker

Hijacker trojans subvert the activating user's connections, redirecting him to other nodes—typically nodes loaded with spam, porn, or extremist political media. The trojan may occasionally redirect the user's connection attempt to a different site, or it may always open an additional second connection every time the user opens one.

### Proxy

This trojan installs a secret proxy server (p. 104) on the user's node when it is activated. If the user's privileges allow for this, it is automatic; otherwise the trojan rolls Rating x 2 (10, 1 Initiative Pass) to install it. The trojan then keeps the server hidden using Rating x 2 to oppose any Matrix Perception Tests. If successful, the proxy server details are immediately transmitted to the trojan's deployer.

### Puppeteer

Puppeteer trojans are designed to aid a hacker to spoof commands. When activated, the puppeteer informs the deploying hacker of the infected user's access ID (if this changes, the trojan will update the hacker), enabling the hacker to more effectively spoof commands from the user. More insidiously, however, the Puppeteer opens a channel by which the hacker can send commands to the trojan, which then resends the commands as the infected user (and with the user's access privileges) to any drones, agents, or devices under the user's command. Because these commands are "legitimate" (coming from the authorized user's account), they are automatically accepted.

### RAT

An abbreviation for "remote access tool," the RAT is designed to immediately install a backdoor within the node when it is activated. Roll its Rating x 2 to create a reusable exploit, a legitimate account, a hidden account, or a hidden access point (see *Backdoors*, p. 99). If successful, the backdoor details are immediately transmitted to the trojan's deployer.

### Sapper

Sapper trojans feature coding similar to the Disarm program (p. 111). When activated, they remain hidden in the node until they receive an activation code from the deploying hacker. At this point, they attempt a Disarm action (p. 112) to neutralize the Firewall against the hacker, rolling Rating + Disarm.

### Vector

When activated, Vector trojans immediately open a connection to download and install a virus, worm, or agent from a predetermined Matrix site. Vector trojans are a common method used to spread malware infections to other nodes. Hackers sometimes use Vector trojans as a clandestine method to sneak an agent onto a target node. Agents and worms downloaded this way operate with the activating user's access privileges.

## TACTICAL AR SOFTWARE

Tactical AR software features sophisticated expert programs designed to analyze a situation, evaluate threats, incorporate sensor data from networked team members, calculate probabilities, run background simulations, and suggest courses of action. Based on previous generations of implanted tactical computers and new systems designed for biodrones (see p. 152, *Augmentation*), these programs incorporate augmented reality, mobile wireless devices, simsense, and advanced sensor technology to maximize tactical capabilities and threat response. Tacnets are commonly used by

| Malware | Availability | Cost (up to Rating 3) | Cost (up to Rating 6) |
|---|---|---|---|
| Trojan | (Rating x 4)F | Rating x 1,000¥ | Rating x 2,000¥ |
| Virus | (Rating x 3)F | Rating x 500¥ | Rating x 1,000¥ |
| Worm | (Rating x 5)F | Rating x 2,000¥ | Rating x 5,000¥ |

military and police units, professional sports teams, emergency services, shadowrunners, and occasionally other scenarios where real-time team networking is crucial.

## TACTICAL NETWORKS

To an individual, tacsofts can sometimes offer interesting advice, but they really thrive when used in a networked environment. They are designed to pool information from team members, assess the overall situation, and coordinate a more effective response with split-second AR data feedback.

For a tactical network to function effectively, it requires a minimum of 3 members. Each member must be running tactical software of an equivalent rating (if the ratings are unequal, the network functions according to the lowest rating software) and must be subscribed to the tactical network (taking up one subscription). Members may be characters running the tacsoft on their commlinks or drones running the software on their systems.

Tactical software has a maximum rating of 4. You may only be part of one tactical network at a time.

### Sensor Channels

Tactical networks rely on data supplied in real-time by sensor systems to maintain an up-to-date model of the tactical situation. In order to function effectively, a minimum of sensory input is required from different sources, measured in the form of sensor channels. In order to be counted as a member of the tactical network (and to receive bonuses from it), each member must contribute a number of sensor channels equal to the tacsoft rating x 2.

Sensor channels are defined as any type of sensory input that can be transmitted to the tactical network (and that contributes in some way to analyzing the tactical situation). Each sense or sensor accounts for a separate sensor channel. This sensory input could include:

**Natural Senses:** Visual, audio, or olfactory senses recorded via simrig each count as a sensor channel. Natural enhancements such as low-light and thermographic count as additional senses.

**Cybernetic Senses:** Any visual, audio, olfactory, or other sense acquired via cybereyes, cyberears, olfactory booster, orientation system, etc. Sensory enhancements such as low-light, thermographic, smartlink, ultrasound, radar, spatial recognizers, and so on each count as a separate sensor channel.

**Sensor Systems:** Data acquired from worn, carried, or mounted sensor systems of various types (cameras, microphones, range finders, motion sensors, etc.) may also be contributed to the network as a sensor channel. Drones sensor systems also count; each drone can supply a number of sensor channels equal to its Sensor rating.

*Brimstone's team is running a Rating 3 tactical network. To count as a contributing team member (and thus to receive bonuses from the network), Brimstone must contribute at least 6 sensor channels. Luckily, Brimstone is a cybersamurai with her share of senseware. Her cybereyes (channel 1) are enhanced with low-light vision (channel 2), smartlink (channel 3), and vision magnification (channel 4). She also has an orientation system (channel 5) and has strapped on an ultrasound sensor (channel 6). All of these sensor systems are linked to her commlink, where she is running her tacsoft, which shares their input data with the rest of the team via tacnet. If for some reason one of her sensor systems was knocked out (for example, she dropped her ultrasound sensor), she would lose a sensor channel and would no longer count as a member of the tacnet team.*

### Centralized Tacnets

The decentralized network structure of traditional tacnets works well for urban combat situations. Under some circumstances, however, a team may prefer to adopt a more centralized model, where the tactical soft is run on a single commlink, which effectively rides in a command and control position. In this situation, the other team members do not need to run their own tacsoft, but they must slave their commlinks to the master node (see *Slaving,* p. 59). Each slaved node takes up 1 subscription slot on the master node's persona (see *Subscriptions,* p. 55). This has the advantage of protecting the network against hacking (especially if the team's hacker runs the master node), but also carries the drawback that the network will fail if the master node is somehow taken out.

## TACNET BONUSES

When in operation, tacnets provide dice pool bonuses for certain actions. The dice pool bonus is based on the number of team members (that is, each member that is supplying the minimum amount of sensor channels). The bonus equals the total number of team members minus 2 (you need at least 3 members to have an effective tacnet, so the first two don't count), up to a maximum equal to the software's rating. So a team running Rating 4 tacnet software with 7 team members gets a dice pool bonus of +4 (the maximum). A team running Rating 4 with 4 team members gets a +2 dice pool bonus (4 – 2).

Tacnet bonuses apply to any test a team member makes that might conceivably benefit from the tactical soft's analysis, data-sharing, and suggestions. This is subject to gamemaster interpretation, but several guidelines can be applied. First, the test's environment must fall not only within range of that character's sensor channels, but also within range of the sensor channels of other team members (at least one). For example, if a team is involved in a firefight inside a building, and one team member runs outside, where none of the others can see/sense, that outside character may not get a tacnet bonus on any tests made outside. Second, the test must be something that tactical data and suggestions from the network could conceivably aid. For example, a test to summon a spirit, kick down a door, or hack a node are unlikely to benefit in any way from the information and resources the tactical network is applying to the situation (for more details on what information tacnets can apply, see *Tacnet Information,* p. 126).

Here are some example tests in which tacnet bonuses might apply:

**Close Combat Tests:** The tacsoft can evaluate fighting styles, stances, opponent's health, and physical layout to instantaneously suggest movement, countermoves, and targeting advice to a character engaged in melee.

**Dodge Tests:** Enemy movement, fields of fire, line of sight, cover location, targeting probabilities, and spent ammunition estimates can benefit a character trying to avoid being hit.

**Firearms Tests:** The tacsoft judges the momentum, speed, and direction of opponents, estimating likely course of movement and probable firefight tactics, giving the user an edge on targeting.

**Infiltration Tests:** Tactical networks can predict likely locations of guards, patrols, and sensors, and evaluate the best course of action contingent to layout and security protocols, in order to assist a sneaking character.

**Maneuvering Tests:** The tacsoft considers maps, environmental factors, speeds, and probable vectors of other vehicles, suggesting maneuvering solutions and other options for vehicles engaged in combat.

**Perception Tests:** Sensor data from other team members can enhance a character's situational awareness.

**Shadowing Tests:** Using motion analysis on a target and analyzing avenues of movement, as well as coordinating multiple scouts, the tactical soft can aid efforts to tail a target unnoticed.

**Surprise Tests:** The tacnet can monitor for signs of ambush or enemies maneuvering to engage a team member unaware.

### Optional Rule: Initiative Bonuses

An optional rule provided under *Augmented Reality,* p. 225, *SR4A,* stated that networked characters could use their network and augmented reality to gain a tactical advantage, possibly including dice pool or Initiative bonuses. These tacnet rules supersede that suggestion with the dice pool modifiers they apply, but they do not offer an Initiative bonus unless you adopt one of the following optional rule options.

The first option is to provide a tacnet Initiative bonus only to characters who access tacnet data via a direct neural interface (DNI), as the information is channeled direct into their brain and accessed that crucial split second more quickly. This would include those linked to their commlinks via datajack or trode net, who have implanted commlinks, or who view the data via cybernetic image links. It would not include characters who view the tacnet's AR data via contacts, glasses, and the like. In game terms, DNI-based tacnet users receive a +1 Initiative bonus (in addition to other tacnet bonuses).

The second option is to allow any character who is part of a tacnet to eschew tacnet dice pool bonuses for a full Combat Turn in exchange for an equal Initiative bonus that turn instead. In this scenario, the character is using the overall tactical awareness provided by the network to plot a general course of action, getting a significant Initiative bonus as a result, rather than reacting to the situation on a play-by-play basis (which would normally award the tacnet dice pool bonus). So a character who might normally have a +3 tacnet dice pool bonus to look forward to can instead take a +3 dice pool bonus on his Initiative Test that Combat Turn.

### Indirect Fire

Using targeting data supplied by another team member, tacnets can be used to engage unseen targets with indirect fire (see *Indirect Fire,* p. 162, *Arsenal*). Similar, networked characters can engage in sensor targeting (see p. 171, *SR4A*) for other members of their tacnet engaged in vehicle combat.

## TACNET INFORMATION

Apart from the dice pool bonus and other benefits, players and gamemasters should keep in mind that the level of interaction tacnets provide, via the exchange of sensory information, first and foremost allows players and characters to coordinate their actions as if everyone part of the tacnet can sense what the other characters sense. Gamemasters especially should keep this in mind when describing the situation to the players and when calling for Perception Tests, as each character's perceptual range is effectively expanded and magnified.

While the sensor channels input by each team member are a crucial source of data, they are not the full extent of the information that a tacnet can supply. The critical part of tactical software is in fact its analytical engine, which is capable of using those sensor feeds to model a situation, make predictions, analyze outcomes, and so forth. This information is then supplied to each team member, along with an ergonomic and data-packed AR interface that highlights the most important data while also making it easy to access other information.

For example, tacsofts can analyze a character's actions in combat to ascertain whether they are friend or foe, color-code

them and plot them on a three-dimensional map or visual display, and assign them a threat rating as to how dangerous they are to each particular team member, even highlighting the ones that are the most immediate threat in a given moment. They can track the probable locations of opponents who have moved out of sensor range, anticipate opponents' actions, and even calculate probabilities for different actions and outcomes. If desired, they can display ballistic trajectories, lines of sight, fields of fire, and blast radii.

Tactical softs are designed to spot and analyze weapons, armor, and other combat factors. Their programming includes built-in databases of weapon, armor, and implant designs and schematics, making it possible for a team member to call up the specs on an opponent's hardware. If something is not listed in its database, they can look it up online, provided there is an active Matrix connection. They can analyze acoustics to determine direction and caliber of the weapon, and count spent ammunition. To judge exactly what a tacsoft spots or knows, the gamemaster can make Perception Tests using Response + tacsoft rating. If the tacsoft needs to search for something online, it rolls tacsoft rating + Browse.

Tactical softs can also take advantage of auxiliary input, such as floor plans or mapsofts, GPS positioning via commlink, sensor software (see p. 60, *Arsenal*), or external sensor feeds that are patched into the network. Team members with biomonitors can also feed that data to the network, allowing their teammates to remotely check their health and vital signs. Spiders are particularly valuable to tactical networks, as they can plug in data from their rigged security systems, giving team members access to interior sensors and possibly even building controls (if the rigger allows it—most will not, preferring to exercise control over their domain).

## SOFTWARE BUNDLES

While programs are the bread and butter of software manufacturers these days, there is always the demand to keep the market alive with new package offers, functional upgrades, and improvement of programs by options or making them less impacting on smaller computer systems. Learning from cybertechnology's take of integration and optimization, program packages, software suites, and skillsoft clusters have become a latest market trend in the software field to persuade the customer to replace their old programs with new ones.

### PROGRAM PACKAGES

Program packages are usually special offers made by software companies to customers buying new commlinks/nodes. They typically include legal programs, agents, and sometimes specialized software as a package deal with a 10–20% discount on the total price.

**Eastern Tiger Palladium**
**Programs:** Armor 4, Biofeedback Filter 3, Medic 3, Track 4

Eastern Tiger offers some defensive utilities in their Palladium package deal, designed for freelance spiders and Matrix security specialists that go one-on-one with intruding hackers or worms.

**Eurosoft Clavicula**
**Programs:** Decrypt 5, Encrypt 5

The Clavicula is a high-end software package featuring excellent encryption and decryption routines from one of Renraku's premier software manufacturer.

**FTL Matrixware Net Wizard**
**Programs:** Analyze 3, Browse 3, Command 1, Edit 2, Purge 3

The Net Wizard is a basic package that includes the most common program needed by a run-of-the-mill Matrix user. Perfect as a starter package to go with new commlinks.

**FTL Matrixware Power Suite**
**Programs:** Analyze 3, Browse 4, Command 2, Edit 4, Purge 4, Scan 2

Another NeoNET-subsidiary starter package, this one marketed towards more advanced Matrix users, business professionals, and the wealthy.

**Pocket Hacker**
**Programs:** Agent (Pilot 3, Browse 3, Exploit 3, Stealth 3)

Released by the notorious Hacker House, this illegal program package is intended for someone who needs a hacker, but doesn't know how to hire one or doesn't want to use a real person.

**Singularity Seeker**
**Programs:** Browse (Crashguard) 5, Browse Agent (Pilot 3 with Browse 3)

This package from a Horizon subsidiary earned solid reviews for its reliability and intuitive search interface, including a search bot of moderate quality.

| Tactical Software | Availability | Cost |
|---|---|---|
| Tacsoft (Rating 1–4) | Rating x 5 | Rating x 3,000¥ |

| Program Packages | Availability | Cost |
|---|---|---|
| Eastern-Tiger Palladium | 6R | 6,640¥ |
| Eurosoft Clavicula | 10R | 4,700¥ |
| FTL Matrixware Net Wizard | — | 480¥ |
| FTL Matrixware Power Suite | — | 1,240¥ |
| Pocket Hacker | 10F | 4,920¥ |
| Singularity Seeker | 4 | 8,200¥ |

## SOFTWARE SUITES

Software suites are combination programs. They incorporate several different programs coded by one particular software manufacturer (commercial or independent) under a single master program interface that offers control over all of the program functions. While software suites are more economic in terms of cost and processing power, they are often more vulnerable to crashing attempts. In game terms, software suites only count as one program when calculating for processor load (see p. 48), even though they consist of two or more programs. If any part of the software suite is infected by a virus or crashed, the other programs in the suite suffer the same fate.

Software suite source code can be programmed, cracked, or patched like any normal software (follow the rules for each component program, however all changes must be done together).

### Homewrecker

**Programs:** Crowbar (Attack 3 with Shredder), Molotov (Attack 3 with Area, AP 2)

Programmed by the famous combat hacker known as Pistons, the Homewrecker is a multi-weapon, multi-option software suite designed to bring down the opposition in a normal node with brute force tactics.

### Iris Antivirus

**Programs:** Analyze 5 with Viral Resistance 3, Purge 5 with Viral Resistance 3

This antiviral suite is designed to detect and purge virus-ridden software. Created by another NeoNET subsidiary (via Transys), this suite is widely regarded as one of the best on the market.

### Shamus

**Programs:** Browse 3, Exploit 3, Sniffer 4

Cranked out by a Peruvian software manufacturer, it is rumoured that this snoop suite was originally developed by KSAF spiders who sold the suite to the South American company due to restrictions imposed on selling restricted software by non-AA companies in North America.

## SKILLSOFT CLUSTERS

Skillsoft clusters are merged skillsoft recordings, meshed together in post-production. These are standardized know- and activesoft packages designed for chipped or skillwired consumers, be they corporate employees, security personnel, or the average customers off the street.

Gamemasters are encouraged to develop their own skillsoft clusters, as best fits their campaigns. Skillsoft clusters have a 20% package cost reduction. When calculating their impact on skillwires, subtract 2 from the total ratings of the skillsoft components. Once bought cluster skillsofts cannot be upgraded or equipped with program options.

### DocWagon Paramedic

**Skillsofts:** DocWagon Procedures 3 (Know), First Aid 3 (Active), Medicine 2 (Active)

Due to the lack of properly trained medical personal in many economically-depressed or conflict areas, DocWagon recently released the Paramedic skillsoft cluster, enabling cybered citizens to act as ad-hoc medics.

### Knight Errant Self-Defence

**Skillsofts:** Dodge 3 (Active), Unarmed Combat 3 (Active)

Originating from a Knight Errant tactical training program, this cluster was co-developed by Ares and Evo to be compatible with the *Versatile Operative™* cyber suites that Evo presented recently on the Cyber-Expo for special assignments that include a skillwire system.

### Manadyne Archmage

**Skillsofts:** Arcana 3 (Active), Magic Background 2 (Know), Latin 4 (Lingua)

This skillsoft cluster was designed with the modern awakened technophile customer in mind. It includes extensive knowledge of magic theory, arcane practices, and mystic traditions, combined with a linguasoft for a so-called "dead language" popular in certain traditions (usually Latin, though variants with other languages also exist).

### Mitsuhama Home Mechanic

**Skillsofts:** Automotive Mechanic 3 (Active), Hardware 2 (Active), Modern Vehicles 3 (Know)

Designed for type of person who would like to fix their own

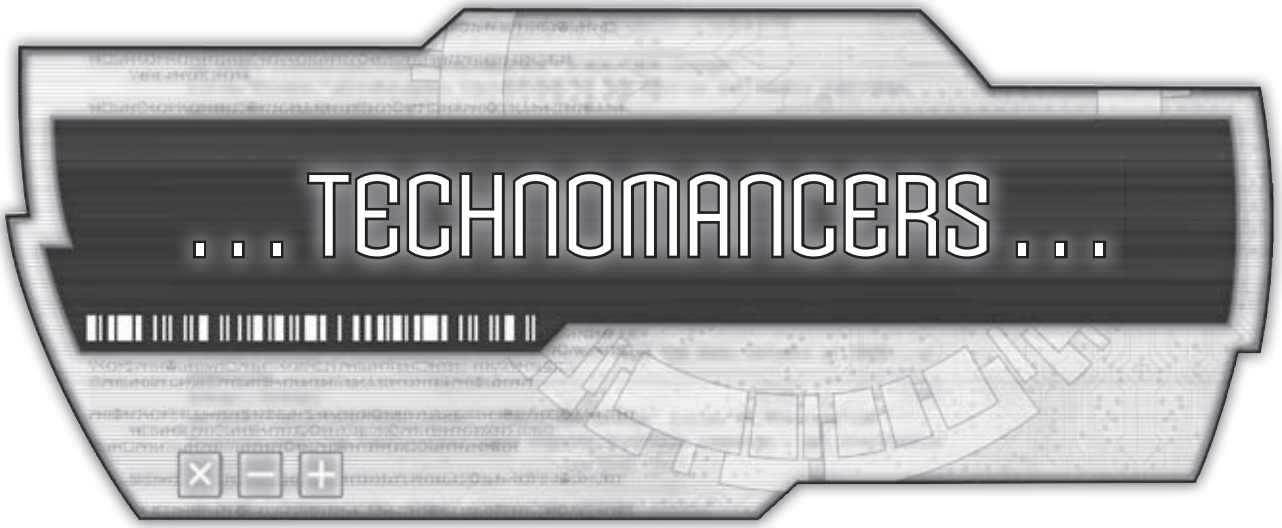
### Whiskey Noir

**Skillsofts:** Forensics 4 (Know), Intimidation 3 (Active), Shadowing 2 (Active)

This skillsoft cluster was designed to a supplemental suite for investigators, consisting of a suite of inquisitive and social skills that come in handy for detective work.

| Software Suites | Availability | Cost |
|---|---|---|
| Homewrecker | 12F | 6,000¥ |
| Iris Antivirus | — | 1,500¥ |
| Shamus | 6F | 5,500¥ |

| Skillsoft Clusters | Availability | Cost |
|---|---|---|
| DocWagon Paramedic | 6 | 44,800¥ |
| Knight Errant Self-Defence | 8 | 48,000¥ |
| Manadyne Archmage | 8 | 28,800¥ |
| Mitsuhama Home Mechanic | 8 | 48,000¥ |
| Whiskey Noir | 8 | 46,400¥ |




The security guard gave Jinx a suspicious look. She watched calmly as he ran her ID a second time, frowning when it passed again.

"This facility is EM-restricted. You must surrender your commlink and all other networking electronics. Any attempt to—"

"I know the drill," she said, handing over her commlink and a few other gadgets. The guard gave her a don't-backtalk-me-bitch look and waved her into a scanner corridor. She noticed that his right hand never wavered from near his firearm. *Guess my corporate drone look isn't so corporate after all.*

"This scan will detect all cybernetic implants, concealed weapons, and wireless-enabled electronics. If there's anything you'd like to declare as contraband, please do so now." He paused, as if he actually expected her to admit that yes, she was armed and dangerous. *Yeah, right. Too bad I'm not.*

He continued his bluster. "It will also fry any arphid tags and detect your EM emissions if you are an unregistered technomancer."

*Thanks for the warning,* she thought, gritting her teeth at the effort of keeping her living persona in play-dead mode. She waited the scan out, then flashed the guard her sweetest smile as she sauntered into the facility. She couldn't see the wireless-inhibiting material built into the walls, but she knew it was there.

She took her time stalking the halls, making it look like she belonged there and knew exactly where she was going. The effort of running silent was killing her. Her skin crawled. Her brain *itched.*

Finally, she reached her destination: an out-of-the-way storage room, hidden from cameras in a low traffic spot. It was guarded by a simple but effective maglock. Her mind cried out, wanting to reach through the ether and caress it, but she didn't dare. *No emitting,* she reminded herself. *They're keeping too close an eye on radio transmissions inside the facility. Good thing I don't need to.* She reached her hand out and touched the maglock, calling up an echo of the Resonance in her mind. Her skin's bioelectric field permeated the device, creating a connection. She *felt* it.

The maglock's AR interface came to life in her mind's eye. The device was slaved to the security nexus—exactly where she wanted to be. Her complex forms sprang to life, pulsing small waves of Resonance at the firewall, feeling for its weak spots and flaws. It was strong, and she could feel its electronic gaze seeking her out, hoping to transfix her with its digital spotlight. It closed in. *There,* she thought. A minor crack in the firewall's code. A programming error, creating a loophole to be exploited. Her complex forms reached in and widened the hole. She was through.

Still standing in the side corridor, touching the maglock, her biological radio muted, Jinx was in. She mentally surveyed the chokepoint node she had penetrated without alarm. Her forms took note of spiders and IC patrolling the system. So far, she remained invisible to them.

She called up, Gizmo, her sprite, who appeared in a burst of glyphs and code fragments. "We have thirty seconds before the team strikes," she motioned to him. "Let's trash this place."

• I know that Netcat's rep score took a bit of a plunge when she revealed herself some time ago, but I don't think there's any better source on technomacers aside from technomancers themselves. I have approved two others to this Jackpoint discussion to provide some alternate viewpoints on the matter. Please welcome undernet guru Otaku-Zuku and Inbus, a technomancer who is working for Technicolor Wings. Let's hope this discussion soothes some of the wounds generated over the past year.
• FastJack

## EMERGING

**Posted By:** Netcat

*"How is it, being a technomancer?"*

I have been asked this question numerous times since my "coming out." Even if you haven't asked it openly, you're probably wondering what it is like being a walking commlink. Though I still encounter mistrust, prejudice, and suspicion simply because of what I am—even here on Jackpoint—I'm paying back a favor to FastJack here by providing a personal report on my Emerging (that's what us technomancers call the event that introduced us to the Resonance, sort of like how magicians refer to their Awakening) and how I experience the real and the digital world.

### BEING IN RESONANCE

The first thing you have to understand is that I never asked to be what I am. I just am. In the years that followed the Crash 2.0, I made peace with myself and accepted that I am different now, that something changed me. I cannot say how it happened, though I can say that the Crash somehow triggered it.

Here's the story. Before '64 I was a student on Matrix technology and system development, though that wasn't my real passion. I was a passionate gamer and as interested in the code as any Matrix freak. I did some small scale hacking and code breaking under the same online handle I still use now—nothing spectacular, though, and definitely not on the level of our hacker wunderkind Slamm-0!

• Don't flatter me. No, just kidding. Continue.
• Slamm-0!

The day of the Crash, I was killing time as I often did, hacking through the levels of *Paranormal Crisis* to obtain some ultra-scarce modifications and gear for an avatar of mine. I don't remember exactly what happened when the Crash hit, but like many others, I was trapped in the Matrix. I have some very faint memories—just a few images and sensations really, plus a fair bit of confusion. Then I came to in an Emergency Room. My roommate had found me slumped on the couch, still jacked in, with static on the display screen. He pulled the plug and got me to a hospital.

It took a few days before I was released from the hospital. I was disoriented for most of that time, and the hospital was overwhelmed with other people who had suffered during the Crash—including dozens who had been trapped online, just like me. The doctors hadn't found any lasting neurological damage they said, so they sent me home with a bottle of painkillers for the non-stop migraine I still had. At this point, I had no idea that my life had changed.

Some weeks and months passed, during which I experienced a few … strange encounters. Sometimes there where whispers as if unseen people were talking to me. Today I know it was the noise and electronic prompts from devices I had unconsciously interacted with. Sometimes I saw things that weren't there, data traffic shaped into images by my brain so that I could understand them. Electronic devices started to function strangely around me. I chalked it on my nerves and post-traumatic stress, trying to ignore it all until the changes were so blatant that I couldn't turn a blind eye anymore. I was confused and frightened, looking for help, but most of the "experts" I visited thought I was a freak, crazy, or overstressed. I started to worry that I was going to be locked away.

• Oh, cry me a river. You can pull our heart strings as long as you want, but that won't persuade me that your kind and your AI allies/creators are *not* a threat to metahumanity. It doesn't matter if you were a hacker before—you're a mutation now, a freak of nature. For me, you are just a ticking time bomb waiting to explode.
• Clockwork

• One very important point that needs to be made here is that not all technomancers were "created" by the Crash. Take me, for example. I was hiking in the mountains when the Crash hit, and didn't even hear about until a few days afterward. Before my Emergence, I never met an AI, never saw a ghost in the machine, never had a run in with Black IC—heck, I never even hacked anything. Then one day back in '68 I was doing maintenance on a drone, running diagnostics on its OS, when I realized my commlink had been accidentally turned off. It confused the hell out of me at first, I couldn't figure out how I was accessing the drone with no 'link. Over the next few weeks, though, I experimented a bit and managed to replicate the situation, and even go a bit further. The day I jumped into a drone, rigging it direct via VR, commlink-free, I knew I was something different. I've heard similar stories from other technomancers—some of them even dating to before the Crash. So don't assume we're a product of the Crash, or manipulated by AIs, or any other such nonsense. If you do, you're just expressing your ignorance.
• Inbus

• The Sixth World has seen many strange things, and I'm sure we'll see even stranger ones in the years to come.
• Icarus

With the installation of the new Matrix and the distribution of commlinks and all kinds of wireless devices, it became worse each week. To walk down a street and have thousands of prompts, data projections, and transmissions raining down on me every second was hard to bear. The more traffic there was clouding the digital ether, the more I had trouble adjusting and dealing with the data flow.

• I imagine it would be much like constant, unstoppable mind reading. If telepaths existed, they would need to learn to shut out the thoughts of any person they interact with or who even comes close to them. I don't envy technomancers, since there is surely a lot more traffic and devices than people. I'm no computer wiz, but I know there are a plethora of processes going on my commlink that I, as a


WARNING!
AUTHORIZED ACCESS
ALERT

user, will never recognize or have to worry about. How do you technomancers deal with that?
• Winterhawk

• It just takes getting used to. Over time, most of us adapt well to filtering out the noise, and actually enjoy the constant hum of activity around us. Meditation helps. Every technomancer has faced the noise problem at some point, and different people develop different coping strategies. For some it is harder than others. Some can't cope at all, and it drives them crazy.
• Otaku-Zuku

• It is like driving on autopilot (non-electronically speaking). When you drive the same way every day, you may suddenly realize that you've been thinking about something and can't remember anything about the past few minutes of driving, even though you somehow navigated traffic without crashing or killing anyone. It happens subconsciously because all the actions and moves are ingrained in your brain, like a program that you just start when starting your car. Well, I've gotten so used to navigating a wireless world that I'm barely even conscious of the traffic around me or how I've interacted with it, though I can easily concentrate and notice it if I need to.
• Inbus

Unlike many technomancers today, I did not have the luxury of having someone on hand who could teach me such things. I was on my own, and I was afraid to tell most people because they wouldn't believe me or would think I was crazy. Everything that I can do today I achieved by myself through training and persistence, and because I had no other choice. I am pretty proud of it. I found my own way.

• A quick aside, from an academic position. As far as current scientific understanding goes, it is not entirely clear how a metahuman biocomputer (read: technomancer) functions and what the source of their abilities is. Genetic predisposition seems to be a crucial factor, and not all individuals who Emerged were trapped in the Matrix or had some sort of previous elevated affinity for the digital word. It is also not an entirely neuronal or bioelectric phenomenon, as far as scientists can tell. The current prevailing theory is that the Emerged are a true evolutionary branch of the human species, just like the Awakened.
• The Smiling Bandit

## EXPERIENCING THE MATRIX

Becoming a technomancer changed my personality unlike any phase of my life before. I am a new person quite different from who I was in the past—not because I am a brainwashed pawn in some global AI chess game, but because of the new experiences and knowledge life forced upon me. Believe me, not all of the changes were easy to swallow.

Unaware at the time that other technomancers existed, and knowing that there was no way I could employ my new skills in the *normal* world, I began looking for more open-minded places where I could rebuild my life and turn my rare talent into profit with enough secrecy to protect myself. I thought the shadows could be such a place, but I was wrong. It was easier to hide what I was, and I did find some acceptance of course. But social marginalization, prejudice, and mistrust based solely on what I am, rather than who I am, are still permanent companions. I don't want to sing my pity song too loudly here, though, as I must admit that previously I never thought much about how about magicians and metahumans may have felt in the 20s or what changelings went through back in '61. It is just the way our society ticks. It is a price I am willing to pay, as my talent has made me special, better than before, and I would not want to live without it anymore.

Before my Emergence, back when I was hacker, I enjoyed spending time in virtual reality worlds. I flew through the clouds, stood in resplendent armor, smelled the fresh spring air, and felt the rays of the virtual sun. It felt real, though my brain always knew it was a simulation. Now, as a technomancer, my daily experience makes those memories seem pale and dull in comparison. Every hacker out there, every normal user immersed in the Matrix right now, experiences but a thin, shallow copy of the world that I sense. What regular Matrix users experience is like looking at an alternate reality through a tinted window. I don't watch the world through this window any more. I climbed through the window and became an active part of the *real* virtual world.

• She is indeed right. Words can hardly describe how much different the Matrix and the real word are to us now. Information pervades our very self, as long as the Matrix is present. It is literally like being attuned to an alternate universe on a frequency that only you can hear. Some would say that we are truly in resonance with the Matrix, we are on the wavelength of the world of information. Most importantly, we are no longer shackled by technology as the rest of metahumanity is.
• Inbus

Though what I "see" of the Matrix is much the same as a standard Matrix user sees—arrows and icons—there is an additional layer of *contextualization* that provides information, sensations, and feelings that was never there before. This extra substance gives me an intuitive sense for what is going on in the Matrix around me. I no longer need to interface with a program or other clunky tools to understand or affect the flow of data around me. I simply reach out and understand what the data is, or what it is doing, and just by concentrating I can change it or make it do other things. I do not need to blink open a window or enter a search routine. I simply visualize the parameters I am looking for in my mind and the Matrix responds to me. I have no use for software any more, not matter how cutting edge—it is a crutch when I can fly. Even hardware no longer interests me, at least as a tool or a possession. Devices are simply extensions of the virtual world to me, charms that the primitives carry around so that they may remain in touch with their ghostly digital world. I have no need for such things, as the Matrix is always with me.

• Every technomancer uses a different method to interface with the Matrix. Imagine an Exploit program. For the hacker it is like sitting in front of a locked door, running a program to probe and find a weak spot to log onto the node. This program will work like a lock picker, trying billions of combinations until it finds the right one (or the blind spot to squeeze through). For me, the Matrix is an overwhelming complex symphony, with each node having his own melody. By

attuning to a particular part of the overall composition, I can whistle myself into the node.
• Otaku-Zuku

**Improvising**

Being a technomancer does not make me a better hacker or a hacker at all. This is a point the media often fails to make when it paints us the bad guys. The Matrix is an environment we feel a connection to, but not all technomancers are node raiders. They are just good with code.

I, however, consider myself a hacking technomancer, which is how I ended up here on Jackpoint. I made myself a reputation for being able to intrude and explore even the most secure nodes. As a normal hacker, I was lousy, but hacking as a technomancer is quite different. A hacker depends on his warez while a technomancer possess the ability to improvise and shape code into a form (something that you would call a program) to manipulate information, something we refer to as *threading*. It still requires skill, but it is by far less technical. It is more artistic, like texturing or throwing pottery, only digital. It is something that gives us an edge over hackers in terms of adaptability, though it isn't a task that is accomplished lightly, and it can in fact be quite exhausting.

**Sprites**

Most people seem to view sprites as spontaneously generated software constructs or agents, which is not giving them the credit for what they truly are and what they are capable of, even if it is a correct designation. Sprites are far more intelligent and sophisticated than any mook I have ever seen. They might possibly be on the same scale as an artificial intelligence, though you can never be sure. The first time I encountered one, compiled subconsciously by my own ability to create them, it scared the shit out of me. While I know that some technomancers view them as pets, companions, or even digital friends, I am cautious when dealing with them. They are a useful bunch nevertheless.

• Don't ever underestimate sprites. I've seen a sprite rip a node apart and kick serious ass. They have some nasty tricks up their sleeves that cannot be copied by any program I am aware of.
• Pistons

• From what I have gathered, the relationship between sprites and technomancers seems very similar to that between spirits and magicians. I have even heard some technomancers refer to sprites as the true spirits of the Matrix, which makes we wonder how close technomancers and magicians truly are.
• Ethernaut

• It may not surprise you that there are also wild and free sprites that dwell in the Matrix. They are rarely encountered, even scarcer than technomancers themselves, but they do exist, roaming the deep virtual spaces. It seems that the virtual landscapes and sculpts have become quite populated since Crash 2.0—as if some gates have been opened, that were closed before.
• Puck

• Pandora's Box, anyone?
• Clockwork

## RIDING THE STREAM

• To pour some oil into the fire of the discussion, here is an interesting report I came across from a neuronal research centre in Geneva, where scientists of the recently formed UNIDS (United Nations Initiative on Digital Sapience) study the technomancer phenomenon on a small group of (voluntary) subjects. I am just adding the highlights.
• Sunshine

**// begin attachment //**
**From "The Diversity of the Virtuakinetics Phenomenon," UNIDS (Draft Report)**

Tests have proven that the four volunteers are truly technomancers. While they seem to possess the same general abilities, there seems to be surprising differences in how they view their abilities, the origin of their powers, and how they make use of them.

**Volunteer 1 is a 45-year-old male Caucasian human.** His psychological profile incorporates a strong faith in God and the conviction that his actions are guided by a higher force, which is why he wanted to volunteer for the program. During his examination, he explained that he acquired his powers via the will of God, whom he claims to have plans for him. In his theistic view, the Matrix is a manifestation of God in the world—in other words, God is the source of his abilities. Volunteer 1 claims to use those abilities in a way that is determined by God's plan. Neuronal imaging of Volunteer 1 while using his technomancer abilities detected activities in cerebral areas normally associated with social interactions. When observed online, he appears to exchange information with computer systems in a very unconventional way. Unlike an ordinary user, he does not actively "use" programs, but rather "asks" or "persuades" computer systems or sprites. This behavioral pattern seems to be innate to his personality and his personal view of his abilities and their origin. Whether educational or age-related factors also play a role here remains to be seen.

**Volunteer 2 is a 15-year-old female Asian human.** Her psychological profile shows a moderate escapism, iatrogenic by a long-term reconstruction gene therapy. During her initial examination, she repeatedly stated that she wanted to go home. She did not refer to her parents' home, however, but the Matrix. She considers the (fully-immersive) Matrix to be her natural habitat, which is quite unusual even among technomancers. From what we could gather during the talk and during interview with the girl's parents, she lives most of her life in a virtual room. She attends school via telepresence, spends all of her time with friends and sprites online, and only leaves virtuality sporadically to eat food and eliminate waste—to the point that she has developed an eating disorder. In regards to her special abilities, neuronal imaging detected no further anomalies. However, her Matrix creations were hyper-realistic in quality and much more detailed than those created by the other volunteers.

**Volunteer 3 is a 35-year-old male Caucasian elf.** He was arrested for tampering with the systems of the drone factory in which he was employed as a janitor and transferred to us from corporate authorities to participate in our program. Despite some sort of fetishism for anthroform robots and drones, Volunteer 3 can be considered harmless. Interestingly, his new abilities seem to have deepened his relationship to drones. Judging from data that we received from the authorities, Volunteer 3 owned a plethora

of robotic toys (including an anthroform companion in which a sprite could be detected), which he had all named and treated as companion pets. While using his abilities, we detected some remarkable neuronal activity in regions usually employed for rigging. Additionally, he was able to display some impressive tricks with drones and machines on the testing ground.

**Volunteer 4 is a 40-year-old female Afro-American dwarf.** Her psychological profile shows a severe lack of emotional responses, almost to the point of suppression. Her mind is strictly organized. Logic governs her responses to all situations, even dealing with trauma-like injury or shocking input. Of all four subjects, she seems the most rational, viewing her abilities as an unusual skill that enables her to deal with the source code underlying the technical operations she conducted in her role as an engineer at a local power plant. She refuses to think of her technomantic abilities as something special, claiming she was just able to "program code on the fly real fast." Even though she Emerged during the Crash 2.0, her gift was not discovered until very recently. Volunteer 4 shows amazing cognitive ability and scored excellent results in all tests.

Based on our knowledge on the traditions of magicians, it can be concluded that the different philosophies displayed by these technomancers are possibly an analogy to those traditons. If that is case, we are not only dealing with one class of technomancer, but with a diversity of virtuakinetic traditions.
**// end attachment //**

• Though I think they're making an interesting point—that both magical traditions and technomancer practices are influenced and even shaped by the practitioner's worldview—I'm not sure that I would agree they are the same. Most magical traditions have developed from long-lasting cultural customs and religious praxis, developed over centuries. Some might even claim that these traditions date back to previous ages of magic! Technomancers, on the other hand, seem to lack that cultural grounding.
• Glasswalker

• Sez you. I fully expect to meet technomancers who recite code in Klingon, worship sprites that look their fave idoru, and experience the Matrix through their personal Neil the Ork Barbarian reality filters. The Matrix is so bloated with "culture" that makes me want to gag.
• Slamm-O!

• Though technomancers may not have the weight of *tradition* to ground their philosophies, the differences in outlook are no less severe—though given their newness, it may take some time for those differences to become clear. One example of how deep their beliefs range, however, is the differing viewpoints on the metaphysical (meta-digital?) source of Resonance. Some believe in a Deep Resonance, others believe in an Architect, where still others worship spirits of the machine. Given time, I'd expect these and others strong currents of technomancer philosophy to develop into unique and individual branches, much like magical traditions.
• Winterhawk

• This is already happening. My blog, the *Undernet Prophet,* became a meeting place for technomancers of all stripes when our existence was made public. Technomancers from all over the world have gathered there, and many of them wield their abilities in ways that I do not. Lacking a term for our distinctive styles (the term "tradition" seemed too shopworn and inappropriate for such a recent phenomenon), some technomancers began using the phrase *"riding the stream"* to express their differences in philosophies. *Cyberadepts* like Netcat and I and *technoshamans* like those that run KivaNet seem the most prominent, though there are many more.
• Otaku-Zuku

• For what it's worth, I consider myself a vehicle empath, though a lot of my kind refer to themselves as dronomancers.
• Inbus

## RESONATING SHADOWS

**Posted By:** Inbus

Although the mass witch hunts have declined, the corps still desire to turn our insides to the outsides, to cut us open in order to understand how we tick—so they can exploit our talent for their own machinations. With a choice of being hunted or shunned, many of us have chosen a third path: taking to the shadows.

• This is an exaggeration. Thousands of technomancers live unmolested normal lives—especially if they remain discreet. Many thousands more have embraced what they are and sold themselves into corporate service. If you believe that there are no technomancer spiders, you are quite mistaken.
• Puck

There are many examples of how one could make a living with our skills and special gifts, but most of them involve keeping our abilities a secret, masquerading as hackers instead. Even among the shadows there are people who won't work or even deal with us because they fell for the lies and misinformation that the corporate propaganda machine disseminated. Fortunately, there are those that appreciate the assistance we can provide, virtually and also physically on the spot. Although we have our limitations when it comes to securing a team's networked defenses, in terms of programs and hardware, our complex forms and sprites can stand up to tough opponents. Our greatest advantage is, of course, our versatility and adaptability, which is one of the reasons why Technicolor Wings hired my talent.

• I had someone call me a Swiss knife of the Matrix, since I am able to adapt to situations I was not prepared for in a very short time just by improvising.
• Netcat

I am wiz with drones and machines, and I can bring out the best of them, when it is necessary. Plus I can play hide and seek with border sensors, which is why they also like me around when we do a border shuffle with some smuggled goods. The same is true for technomancer hackers, who excel at intrusions, data sniffing, and shaving IC. Sure, a regular hacker or rigger could do my job, but we technomancers (and our sprites) have a few tricks up our virtual sleeves that they could never pull off.

# ADVANCED TECHNOMANCER RULES

The recent events that dragged technomancers into the media spotlight—generating globe-spanning mistrust and witch hunts, but also strong support—made the existence of technomancers public knowledge. Although technomancers still encounter prejudice and caution because of who they are and what they can do, many different organizations (corporations, scientific groups, and transhuman societies) are taking a great interest in technomancers, especially when it comes to their unique ability to manipulate electric fields and processes in the Matrix with their minds.

As technomancers come out of hiding, research and experience have provided more insight into how their abilities work and how they can develop their powers. It has become evident that the evolution of the *electro-sapiens* is far from over.

This section provides new rules and expanded definitions for technomancers and technomancer abilities, based on the rules introduced in p. 239, *SR4A.*

## THE BIOLOGICAL PAN

Since technomancers are essentially organic computers with neural and bioelectric wiring (including a sim module), they form their own nodes when interacting or interfacing with the Matrix or other electronic devices. This "biological node" is part of the technomancer's living persona and is characterized by the four Matrix attributes: Firewall, System, Response, and Signal (p. 239, *SR4A*).

Unlike peripherals, standard nodes, and nexi (*Nodes*, p. 55), biological nodes are not "places of the Matrix" with addresses and access ID numbers, and can neither run programs nor store data. They are visual and virtual representations created by the technomancer himself as subconscious aids to deal with data transfers, "node scripts," and subscription of wireless devices.

### Connecting

When a technomancer goes online, his living persona acts as a biological commlink and routes his connection requests, data transfers, and other traffic through the nearest wireless node within his signal range to the rest of the Matrix. Since technomancers don't have hardwired access IDs, they automatically spoof one (see *Spoofing*, p. 236, *SR4A*) without needing to perform any tests.

### Modes and Scanning

The organic node of technomancers is always considered to be in hidden mode; they cannot operate in active or passive mode. Biological nodes are difficult to detect with standard wireless node scanning, as they do not follow standard wireless device acknowledge-response protocols. They do emit radio signals, however, so they can be located in the same way as a node in hidden mode (see *Detecting Hidden Node,* p. 230, *SR4A*). A technomancer who wishes to "run silent" can shut down his radio emissions, making himself undetectable to radio scanners, though most technomancers find this state to be uncomfortable, especially for long periods. He can also go into "receiver mode," which allows him to receive radio transmissions and still remain undetectable to scanners, but this disallows any connections that require a subscription (keep in mind that most data transactions are two-way).

Technomancers are as prone to jamming (p. 231, *SR4A*) as any electronic device.

### Tracking and Hacking

Like mobile wireless devices, the biological node of a technomancer is difficult to pinpoint with a Track program. At best, the technomancer's current location can be roughly triangulated in relation to a node to which he is connected, and only within its signal range, to within 50 meters (see *Trace User,* p. 232, *SR4A*).

Because commlinks and other electronic devices fail to recognize the biological node as a valid node, technomancers are immune to access connections and hacking by "mundane" spiders and hackers, although they can still be hacked by other technomancers or by sprites (*Hacking the Biological Node*, p. 135).

### Subscriptions and Traffic

Technomancers subscribe and link wireless devices (for example drones) to their biological node as per normal rules. The technomancer's subscription list may be unlimited in size, but the number of nodes, agents, or drones that he may actively subscribe to (access) at any one time is limited to his System x 2; this is the maximum amount of traffic the technomancer's neural infrastructure can handle at once. Sprites don't have to be subscribed by a technomancer.

Although an opposing hacker cannot scan or enter the technomancer's biological node, he can sense and intercept the wireless traffic between the technomancer and an electronic node (like a drone or device) as mentioned on p. 230, *SR4A.* Hackers can even spoof a signal coming from the technomancer, as the traffic originating from the bio-node has to be in an electronic format that devices can understand, and is therefore vulnerable to forgery. Hackers may not, however, spoof commands to sprites (though technomancers may spoof such commands).

### Consciousness

While sleeping, technomancers may decide to stay connected to the Matrix—for example, to receive messages or data from a sprite that was sent on a remote task (p. 241, *SR4A*)—though it makes them vulnerable to counterhacks by another technomancer. At the gamemaster's discretion, an attack or other notable Matrix activity may awaken the sleeping technomancer.

If at any time the technomancer falls unconscious, either in the Matrix or in the meat world, the living persona shuts down just as if someone had switched a commlink. The technomancer will have to reboot per normal rules. Only Black IC attacks have been shown to be able to trap the technomancer online while unconscious (p. 237, *SR4A*).

## HACKING THE BIOLOGICAL NODE

While the biological node is impenetrable to hackers, it is vulnerable to technomancers and sprites, who are "on the same wavelength," wirelessly speaking. Technomancers and sprites can locate and hack other technomancers' biological nodes per normal rules, although one cannot probe a technomancer for weakness. Hacking a technomancer is always considered to be a hacking in on the fly for an "admin account" (+6 threshold modifier).

If the technomancer possesses the Analyze complex form, he subconsciously tries to recognize the intruder. He can send compiled or registered sprites on "patrol" in his biological node. This expends one task. Alarms caused by the technomancer (or sprite) have the same in-game effect as in a normal node, as the technomancer's electroimmune system attempts to shut out the

intruder. The technomancer can also project into his biological node and engage an intruder in cybercombat (and most will).

Note that biological nodes may not be encrypted.

### Matrix Actions in the Biological Node

Since the biological node does not store data as a commlink does, these nodes are commonly perceived as empty (similar to virtual machines). However, since they can enter the node, hacking technomancers can:

- access slaved devices (see *Slaving,* p. 59)
- edit (add or delete) subscribed connections, using Hacking + Edit
- intercept traffic (p. 230, *SR4A*)
- crash the biological node

Crashing the biological node is a painful and unpleasant experience as it forcefully severs all links to the Matrix and forces the technomancer to reboot (p. 231, *SR4A*). In addition, the technomancer suffers a –2 dice pool modifier from disorientation and vertigo until he has fully rebooted.

### Roleplaying Biological Node Hacking

Having your bio-node hacked is an unpleasant experience for any technomancer—it is, in effect, an intruder in your head. Just as the biological node is not a normal "place" in the Matrix, however, it should also not be confused for the technomancer's *brain*. The bio-node is a construct created and maintained by the brain as an extension of their abilities. So while a biological node can be hacked, this does not mean the hacking technomancer can gain any control over the target's memories, thoughts, personality, or actions. Instead, hacking a bio-node is more akin to attacking the root of a technomancer's Resonance abilities.

## ADVANCED COMPLEX FORMS

Technomancers use or create complex forms that mimic programs to assist them in manipulating the digital information of the Matrix. For rules purposes, these are considered normal programs in the way they interact with the Matrix (unless otherwise noted), and they may be crashed just like other programs.

At the gamemaster's discretion, the following new complex forms may be available to technomancers at character creation or may be learned later during the game. They follow all the same rules for complex forms given on p. 239, *SR4A* and within this chapter.

**Complex Forms and Degradation:** Since complex forms are different from normal software, they don't need to be patched up and are immune to degradation (see *Software,* p. 106). They are always at the cutting edge, through the technomancer's contact with the "state of the art" of the Matrix.

**Complex Forms and Program Options:** Options for complex forms must be purchased at a cost of 2 Karma per program option or program option rating (1 BP per option or point at character creation). A complex form can be equipped with a number of options equal to half its rating. For threading of program options, see p. 148. Once an option is purchased, the technomancer can choose whether or not to use that option each time he uses the complex form.

### Shield

Since Matrix damage always affects their living persona directly, technomancers rely on defensive measures more than normal Matrix users. The Shield complex form enables the technomancer to deflect and counter code attacks from combat utilities targeted at him. Each rating in the Shield complex form adds +1 die to the Matrix defense pool.

### ADOPTING SOFTWARE

In theory, a technomancer can adapt any piece of software by mimicking the program with a complex form that he shapes (by threading or learning) based on the original. Since a number of programs such as Sensor software (p. 60, *Arsenal*) or tacsofts (p. 125) require connections to sensors, databases, and/or other auxiliary data, a technomancer can only use complex forms based on that software if he has a connection to such sensors, databases, or auxiliary components. Individual gamemasters may choose whether to allow this in their games.

## NON-RATED COMPLEX FORMS

Technomancers may also mimic non-rated programs with threading or complex forms, such as AR environment software. Two specific options are described here. For Karma cost purposes, treat non-rated complex forms as if they had a rating of 1.

### Simrig

Technomancers can code a complex form that enables them to record their own experiences (both physical and emotive) in form of simsense recordings like a normal simrig (p. 328, *SR4A*) would. Although this complex form allows them to convert the recording into a file format that can be interpreted by any sim module, each recording must be saved externally.

### Smartlink

Although the technomancer's physiology and wireless capabilities enable him to "talk" to smartlinked devices (e.g., exchange data with a weapon and display it accordingly) without any additional devices, he normally lacks the hard-coded tactical software to translate the information into visual cues that simplify target recognition, aiming, and shooting in combat. However, technomancers can simply create this program by learning it as a permanent complex form, or improvise the necessary algorithms by threading.

Treat Smartlink as a complex form with a rating of 1 for all rules purposes.

## RESONANCE STREAMS

Though a technomancer's Emergence is similar in some ways to a magician's Awakening, technomancers do not resort to mythical concepts like witchcraft, shamanism, or other hermetic or esoteric teachings in order to visualize their abilities. For the most part, ancient religions and cultural practices have failed to incorporate the digital realm. Instead, technomancers invented their own new belief systems, referred to by some as *streams,* that seem to offer some answers about their nature and help them find and take a new place in the Sixth World.

Streams are still evolving and are not yet as stereotyped as the paradigms of the Awakened community. Technomancers following the same set of parameters—"*riding the same stream,*" as some say—have started to codify and streamline their beliefs, paving the way for currently Emerging technomancers.

### Rationalizating the Digital Mind

Though many technomancers do not like being pigeonholed or do not easily accept pre-defined doctrines, many of the newly Emerged find it comforting to adopt practices and techniques devised by others that fit with their own ideas and perceptions of the virtual world. As the process of Emergence is a life-changing event, challenging beliefs and turning one's life upside down, individuals who become technomancers often change their outlook and even their personality, which can explain why even the most rational mind might turn into a believer in the mystic nature of code.

### Creating a Stream

To create a new stream, the player must choose the following:

1. The core concept of the Stream.
2. The type of sprites that can be compiled by technomancers riding the stream.
3. The means by which technomancers on the stream resist Fading.

The definition of a stream is vital for a technomancer, as it defines his underlying philosophy, how he reacts to and interacts with both the real and the virtual worlds. While the beliefs of a technomancer stream are less tangible (especially from the role-playing point of view) than magical traditions that are based on known religious or magical concepts, the gamemaster and the player should work together to create a stream that makes sense within the scope of their specific game and the *Shadowrun* universe as a whole.

### Concept

The core of a stream is its philosophy of the Matrix and the Resonance. It is a technomancer's way of explaining how the Matrix changed with Crash 2.0, what Resonance is, and how she can manipulate the processes of the Matrix. While the fundamental belief of a stream has no game effects, it affects the way a technomancer views the Matrix, nodes, and virtual reality. It is therefore important to sketch out a stream's core concepts before detailing how it works in game terms.

Does your technomancer have a natural affinity for the cyberworld, perceiving it as her real home? How is the technomancer's interaction with Matrix processes defined in terms of complex forms? Does she actively force the code to do her bidding or persuasively ask the living Matrix to change as she desires? Does she rationalize her existence as an evolutionary branch that mankind has taken, or is everything the result of higher forces?

Each of these ideas is a stepping stone toward fleshing out how the character perceives herself in relation to both reality and the digital realm.

## OPTIONAL RULE:
*The Resonance Difference*

The way that technomancers, complex forms, and sprites operate—using Resonance—is far different from how standard personas, programs, and agents work. For simplicity and flow, these are often treated the same in terms of game mechanics, and, indeed, this makes some practical sense. For example, complex forms must interact with nodes and standard Matrix programs, and so the complex forms would need to "speak the same language" in terms of input/output and be recognized as legitimate "software," otherwise there would be problems.

Nevertheless, complex forms and sprites are not composed of code in the normal sense, and so it is conceivable that certain actions made against them might not get the same results as they would against typical software. This optional rule provides for this, but gamemasters should be aware that this gives technomancers a certain edge over hackers, and so should apply it careful. Alternately, these options could be handled as echoes.

**Attack Protection**

Normal Attack programs are less effective against technomancers and sprites, as the code faults such software normally exploits are simply not there. Apply a +2 dice pool modifier to the Defense Test against such attacks.

**Difficult to Analyze**

Though megacorps and security companies have made great inroads in identifying technomancers, complex forms, sprites, and even echoes, the nature of Resonance still makes each of these harder to identify—they simply don't match regular code patterns, and the look of a complex form used by one technomancer looks completely different when wielded by a technomancer from a different stream. Increase the threshold for Matrix Perception Tests against technomancers, complex forms, sprites, echoes, and widgets by 1.

**Immunity to Crashing**

Under this rule, the normal routines and tricks that make software vulnerable to crashing do not exist in Resonance-fueled complex forms. This makes technomancer complex forms immune to crashing, unless the Crash action is initiated by a technomancer or sprite. Technomancers and sprites may still crash the programs of regular Matrix users.

**Immunity to Defusing**

For the same reasons, A Data Bomb created by complex form *cannot* be disarmed by a normal Defuse

***Continued on page 138***

**OPTIONAL RULE:**
*The Resonance Difference (CONT.)*

program, though it may be disarmed by a Defuse complex form.

**Immunity to Nuke**

The system resources targeted by normal Nuke programs do not exist for technomancers and sprites, so they are immune to their effect.

**Invisible Node**

Being a construct of Resonance, the biological node is completely immune to standard scanning attempts to detect a wireless node, unless a technomancer or sprite is doing the scanning. In this model, technomancers may run their nodes in active, passive, or hidden mode in relation to other technomancers and sprites.

**Resonance Encryption**

The Encrypt complex form creates a Resonance code that is simply unbreakable to normal Decrypt programs. The only way to break this code is with a Decrypt complex form.

**Superior Trace**

The Track complex form is immune to the confusing signals sent by a Spoof program when a hacker attempts to redirect a trace (p. 231, *SR4A*). Only a Redirect Trace performed with a Spoof complex form can throw the technomancer or sprite off the trail.

### Sprites

Each stream can compile five sprites that represent the focus of the stream to certain aspects of the Matrix. Technomancers always perceive sprites as what they are (as opposed to magicians' views of spirits), even if a sprite looks different based on the stream of its compiler. A fault sprite will always be called a fault sprite, whether it looks like the mechanoid disassembler of a dronomancer, the bio-mecha shredder of a cyberadept, or the virtual cyclone of an e-scapist.

### Fading

Every stream relies on Resonance to resist Fading. In addition, each stream uses one Mental attribute (Charisma, Intuition, Logic, or Willpower) to assist in Fading resistance. The attribute used is the same for all members of that Stream and may not be changed later.

## SAMPLE STREAMS

Two streams, the cyberadepts and technoshamans, have a significant presence in *Shadowrun*, as they were developed by the first Children of the Matrix—the otaku—before the virtual landscape quaked during Crash 2.0. Many technomancers, drawn to the workings of the former otaku, have embraced the basic principles of these paths and shaped them into full-fledged streams. These and other examples of streams are shown below.

### Cyberadepts

**Fading:** Willpower + Resonance
**Sprites:** Courier, Crack, Data, Fault, and Machine
**Note:** The "standard" technomancer described on p. 239, *SR4A,* is part of the cyberadept stream.

The majority of technomancers are cyberadepts, though they may call themselves code-dealers, trix-jockeys, or virtuakinetics. They view their abilities as a natural fusion between metahumanity and technology, fueled by Resonance, which they view as a unique force or energy (e-*Qi*). To them, Resonance is an energy form that must be actively manipulated and controlled in order to affect data and impact the Matrix by the sheer force of their wills. Cyberadepts do not share the spiritual views of technoshamans or info savants, and usually care less about the origin of their abilities and the nature of sprites. They see sprites merely as intelligent tools, animated by Resonance, rather than as beings, and their sprites often take the shape of objects rather than creatures. Because of their pragmatic view of the Matrix—and their frequent egocentric behavior—cyberadepts often use their technomancer abilities in the positions or jobs they had before their Emergence, combining their real-world skills with their virtual ones.

### Dronomancers

**Fading:** Intuition + Resonance
**Sprites:** Crack, Data, Fault, Machine, and Tutor

Technomancers who originate from the Japanese *tekeno-feto* culture, or who possess some other kind of techno-fetishism associated with robots, drones, vehicles, or other electronic devices, are known as dronomancers, puppeteks, or robomancers. For a dronomancer, the Matrix is a world of connected machines that he can talk with. Unlike other technomancers, who are drawn to the code and information, dronomancers are drawn to slaved machines and other electronic devices. Dronomancers see the dog brains of drones and agents as pet-like entities, and sprites as embodiments of the spirits of the machines from which they manifest. Sprites compiled by dronomancers typically display some feature of the object or node in which they are compiled, often appearing machine-like. Because of their rapport with machines, dronomancers enjoy experiencing the world through the electronic eyes (i.e., sensors) of their slaved drones and devices.

### E-scapists

**Fading:** Willpower + Resonance
**Sprites:** Courier, Crack, Data, Fault, and Tank

Not all technomancers are deeply rooted in the real world. With the Sixth World being an inhospitable place for a lot of people in the '70s, some technomancers, called e-scapists or sculptors, consider cyberspace a better world that users can shape into their own utopias. Although still bound by their mortal bodies, e-scapists try to escape reality as often as possible, embracing virtual reality wholeheartedly as the only world where they truly fit in. As the real world becomes a second home (viewing their real lives as virtual avatars like those used in the first decade of the 21st century) with a body that can be easily discarded to venture the depths of virtual reality, e-scapists excel in creating virtual environments and achieving wonders with creativity and imagination. Sprites are envisioned as true companions with their own personalities and tend to take unique forms that are reported to be more "alive" than those of other technomancers.

### Info Savants

**Fading:** Intuition + Resonance
**Sprites:** Code, Courier, Data, Machine, and Paladin

Info savants view the Matrix as a place of wonders. Similar to technoshamans, their approach is more spiritual and intuitive, but they don't believe in higher forces, just in data. Info savants—also called infomancers or datamancers—perceive the Matrix in its raw form as rivers of information that flow in all directions within the endless virtual landscape. People, with their commlinks and PANs, are seen as *information wells* in which consumer habits, interests, and social networking form patterns that info savants can perceive. Some go even further, believing that events in the real world manifest as patterns on the digital, assembling and disassembling depending on the impact of the event and the amount of data accumulated.

Info savants interact with a node by redirecting the virtual chi, using some kind of digital feng shui to alter the flow of data, either with their complex forms or through sprites. They venerate sprites as spirits of the code, calling them and asking them for assistance rather than commanding them into obedience.

Some see info savants as the technomancer version of geomancers, following the digital ley lines of the Matrix.

### Networkers

**Fading:** Charisma + Resonance
**Sprites:** Code, Courier, Crack, Data, and Sleuth

To networkers, the Matrix is a complex digital cobweb, a plethora of threads along which traffic and communication travel in every direction like an electric potential migrating on a nerve. Pervading the modern world, these threads connect and affect every place, anywhere, at any time. Networkers think of themselves as the spiders of these webs, the ones who can truly see and influence its patterns. By spinning new threads or removing old ones, networkers manipulate the web. Some believe that even small changes can lead to far-reaching, drastic changes, based on the Twentieth Century concepts of the butterfly, domino, and snowball effects.

Resonance is nothing but the glue that holds the web together, which the technomancer draws upon when "weaving." Sprites are perceived as "organic" helpers, innate auxiliary programs designed to help technomancers service the web. Networkers' sprites are usually viewed as intelligent Resonance programs (ranking between complex forms and technomancers themselves) without much personality or motivation of their own, They tend to have alien or task-oriented sterile iconographies, often based on the "weaving" metaphor, such as spiders or webspinners.

### Singularitarians

**Fading:** Logic + Resonance
**Sprites:** Courier, Crack, Data, Tutor, and Tank

The technomancers on this stream are convinced that they are the next step in the development that is necessary to transform the living Matrix into a machine super-intelligence (something beyond even previously powerful AIs such as Deus) that will guide mankind through their own evolution. Calling themselves singularitarians or e-volutionsts, they view everyone in the Matrix as a part of this flourishing intelligent supercomputer that will at same point awaken (causing a bigger singularity event than the Crash 2.0) and change

the world on a not-yet-conceivable level. Resonance is perceived as the fabric from which this computer is made, while technomancers, normal Matrix users, and even sprites are self-evolving subroutines that have to learn to increase their abilities and possibilities in the Matrix (over generations) until they have evolved enough to reach the critical level of a singularity.

While singularitarians often have a lot in common with transhumanists, even many transhumanists and technomancers view their philosophy as quite abstract and esoteric, and worry that the singularity will in fact not be friendly to metahumanity.

### Sourcerors

**Fading:** Logic + Resonance
**Sprites:** Code, Courier, Crack, Data, and Machine

Many of those who became technomancers in the wake of Crash 2.0 were ordinary people with ordinary jobs who did not care much about magic or digital mojo before they experienced it themselves during their Emergence. Sourcerors, therefore, deal with resonance in a very rational way, reminiscent of mathematical logic or computer science. Similar to those hermetic magicians who view magic as a physical force with predictable laws and consequences, sourcerors view Resonance as the true machine code of the Matrix, which only they are able to understand. From their perspective, they use complex forms as interfaces to program the machine code. Sprites are thought of as sentient programs, embodied subroutines similar to agents that can be commanded and directed like any other program. Sprites compiled by sourcerors often resemble sculpts of commercially available agent programs.

### Technoshamans

**Fading:** Charisma + Resonance
**Sprites:** Crack, Data, Machine, Paladin, and Sleuth

Technoshamanism is a spiritual view of the Matrix. Members of this stream think of the Matrix as something bigger, something *alive,* a higher being they can communicate with. While some technoshamans are former otaku who believe that Resonance was created by some sort of higher beings or spirits of the machine, many newly Emerged technomancers are attracted to this digital spirituality based on a connection they feel with the virtual world.

Technoshamans have a sympathetic, nearly religious relationship with the Matrix, and often ally themselves with the strange beings that reside within, including new AIs. Wandering the Matrix as digital pilgrims, preachers, and prophets of the living Resonance, their practice of technomancer skills is ritualized, comparable to arcane shamans in the real world. Their methods of compiling and registering sprites often bear similarities with arcane conjurations, and they treat sprites with respect, as natural denizens of the Matrix. Sprites compiled by technoshamans frequently display ethereal or ghost-like features that reflect their otherworldly nature.

Technoshamans usually have a paragon (p. 149).

## IN TUNE WITH THE MATRIX–SUBMERSION

While the phenomenon of Emergence is still young compared to the Awakening, technomancers have displayed fast development in recent years, breaking new ground toward personal attunement with the Matrix and the Resonance. Profiting from former otaku who were willing to share their knowledge about "modes" of submersion, technomancers today are blazing their own paths at virtual speeds.

## TAKING A DIVE

A very personal and ego-wrenching experience, submersion is a process of growth and awareness that forces a technomancer to grapple with her fears, small-mindedness, and shortcomings, opening her mind and developing a deeper understanding of herself and the Matrix.

Since the actual process requires the technomancer to submerge her living persona into the depths of the digital world, some have referred to submersion as "taking a dive" in the virtual sea. By becoming one with the code, the technomancer allows Resonance to seep through her digital essence, which enables her to see behind sculpted iconography and to understand the Matrix on a fundamental level. This intuitive realization grants her access to greater abilities known as *echoes,* and also enables her to use "backdoors" into the Resonance Realms (p. 172) underlying the Matrix.

To follow this path of improvement, technomancer characters must pay the Karma cost of the appropriate grade of submersion and should have spent some time exploring its abilities by interacting with the virtual world.

Gamemasters should carefully consider if a technomancer has gained enough insight to perform a further submersion. It should not be viewed as a fast way to gain new echoes, which can be acquired more easily by using the Optional Rule to Emerge Echoes (p. 145).

The basic rules concerning submersion and echoes can be found on p. 243, *SR4A*. The following rules are intended to provide additional options and depth to the process of submersion.

### SUBMERSION

**Submersion Base Cost:** 10 + (Grade x 3)
**Network Submersion:** Base cost – 20% (round up)*
**Submersion Task:** Base cost – 20% (round up)*

* These may be combined for a net submersion cost of Base cost – 40% (round up)

### Network Submersion

While a character can easily submerge on her own (p. 243, *SR4A*), she may also do so as part of a resonance network (*Resonance Networks*, p. 142). Submerged technomancers with like-minded interests often connect virtually, out of mutual interest and understanding of the Matrix and the Resonance that links them. While some temporary networks (called *parties*) exist just for the joint process of submersion or sharing of knowledge, most networks (nicknamed *guilds*) are stable and long-term associations that provide a basis to share and exchange information and knowledge, even if these guilds only exist virtually.

### Virtual Crossing

Submersion is a breakpoint on an indefinite virtual journey toward a deeper understanding of the Matrix. It is a hyper-real

### WITHOUT A STREAM– WILD TECHNOMANCERS

Emerging technomancers may only gradually realize their true nature. While magic is publicly known to everyone watching the latest adventures of Karl Kombatmage or Suki Redflower, or documentaries and news on the trideo, technomancers lack role models from mythology, history, or even science to rely on. Despite the extensive media coverage and attention technomancers received in 2070, it often takes Emerging technomancers more time to understand the "strange things" they can do and find their own stream in order to deal with those abilities.

Some technomancers, however, may never grasp their special nature or find a stream that helps them control their abilities and channel them in ordered ways. These *wild technomancers* don't have much control over their abilities and cannot purposely compile sprites. Their uncontrolled living personas and erratic interaction with electronic systems and nodes often turn them into unpredictable beings that are a threat to themselves and their environment, especially if they are prone to lose control over their abilities in emotionally intense situations because of fear or anger.

For more details on wild technomancers, see the quality on p. 38.

experience, induced by unfiltered exposure to pure Resonance, by which the technomancer transcends himself to gain a new level of advancement, leading to a "digital evolution" and a spiritual revelation. This process, often referred to as "recoding," enables technomancers to gain access to the deeper layers of the Matrix to spawn echoes.

Since submersion is part of the individual's unveiling of the code and personal transformation, it is an intimate process that is influenced by the character's own views and beliefs. The character's perception of the Matrix, reflected by his chosen stream (p. 136) or paragon (p. 149), should be taken into account by gamemasters and players developing their own "rite of crossing." A technoshaman might go on a pilgrimage to virtual landscapes and nodes he feels connected with; a dronomancer might need to start from a "jumped-in" view of a vehicle or drone; a sourceror might prepare meticulously to open a back door with a gate-like ritual; or an info savant might dowse over a pile of code. Rites vary enormously, depending on stream-specific beliefs and attunements to different aspects of the Matrix.

Except for the basic time and effort required to undergo submersion tasks (see below), the gamemaster is free to adjust the time spent and the submersion event involved to suit the character and the flavor of her campaign. As the Resonance cyberspace is beyond the sense of time, characters could even experience a whole virtual life during a submersion.

If the player desires, the submersion may include a *submersion task* (p. 141). These tasks are specific challenges of will and ability to which the character willingly submits in order to prove himself worthy of submersion.

The paragon of a technomancer, should he follow one, may also play an important part during the submersion session, the preparing task, or both, though exactly what that role is should be tailored to the particular character and the nature of the crossing rite or submersion task he chooses.

While the group's style of gaming may determine how much attention is devoted to submersion sessions, it provides a unique roleplaying and story opportunity that should be emphasized.


## SUBMERSION TASKS

Characters who want to perform a submersion may prepare for it with a *task* that "tunes" them by challenging their focus and ability. This can be an intrusion in a highly secured node on the fly, cybercombat against a coded mayhem, or creating a new piece of code.

Undergoing a task for submersion reduces the normal Karma cost of submersion by 20 percent (rounded up). Only one task is possible per submersion. The character must choose the task before undergoing submersion (or the task must take place 24 hours before the submersion session starts). The technomancer cannot "save up" tasks except for the great hack (p. 142). If the character passes the task he is able to undergo submersion with reduced costs. It he fails, he can either retry (without losing karma) until he succeeds, or pay the full price for the submersion.

Since submersion is a fairly new phenomenon, only a few tasks have so far been discovered by the techomancer community, though more are suspected to show up in the future as technomancers continue pursuing the ways toward digital ascension.

The following submersion tasks are examples commonly known to technomancers. Players and gamemasters are encouraged to design new submersion tasks to fit their story and the technomancer's agenda.

### Evisceration

A virtual sacrifice of some kind, evisceration is a deliberate mutilation of the technomancer's persona that also causes debilitating effects on his real body due to feedback in the technomancer's neurological structure. A technomancer may call on this submersion task and virtually sacrifice a part of his living persona (such as its resolution, its physical appearance, or even one of its limbs). While this "damage" will not impair him on the virtual level, the sacrificed or damaged part becomes neurologically impaired in reality. An arm that was virtually cut off in the process of evisceration becomes numb and paralyzed. Certain areas of the body may turn numb as a result of de-rezzing a persona.

While the technomancer does not lose attribute points as a result of the process, it should impair him in one way or another. The exact nature of the handicap and possible negative dice pool modifier for physical tests is left to the gamemaster, but should reflect a negative quality worth at least 10 BP that cannot be bought off.

### Great Hack

A great hack task requires a character to perform a difficult on-the-fly hack to show her skills to the hacker or technomancer online community. Before committing the great hack, the gamemaster and player should agree on an appropriate target and introduce it through roleplaying. Such a task may develop into a run in its own right (for instance, an isolated node that cannot be accessed from the outside and must be hacked from the inside), though the run must be personally relevant and appropriate to the character undertaking it.

As a general guideline, the Karma award for the run should be comparable to the Karma cost of the grade the character seeks. If the gamemaster approves the run or part thereof as a great hack, successfully accomplishing the goal of the run means the first part of the task is accomplished.

The second part of a great hack is to boost its fame by uploading data acquired during the hack on a public or hacker site, including some sort of tag or logo that refers to the character, to "show off." This is, however, evidence that the character committed the crime ... law enforcement is likely to take notice!

Nodes of governmental agencies, R&D nexi of corporations, bank accounts or private nodes of public or famous figures, as well as other highly secured nodes are common targets for great hacks.

At the gamemaster's discretion, a character may carry out a great hack before she is ready to submerge to another grade, essentially "saving" the hack and using it as a task for her next submersion. A great hack must be used for the character's next submersion, however, and cannot be saved beyond that grade.

### Reassembling

If a technomancer assists an entropic sprite in a reassembling process (p. 158), sacrificing one of his registered sprites and participating in the ritual recoding of the sprite can be used as a submersion task. In order to profit from such a spiritual moment, the character must succeed in an Intuition + Resonance (2) Test *and* a Willpower + Logic (2) Test.

### Resonance Realm Search

To undergo this task, the technomancer must access a specific location on a resonance realm, often referred to as a *resonance room* or *instance*. Only characters who have undergone submersion before can locate backdoors into the resonance realm (*Resonance Realms*, p. 172) hidden in the Matrix.

Before accessing the resonance realm, the technomancer must get access via the backdoor, requiring a Resonance + Fading attribute + submersion grade (12, 1 hour) Extended Test. There is no penalty for briefly interrupting the preparation process, but the process is demanding and leaves no time for any activities other than the most ordinary tasks.

The gamemaster should tailor the search to fit the technomancer's stream and beliefs, not only challenging his hacking skills but making it a drastic and tremendous experience that tests every aspect of the technomancer's personality.

### Source Code

This task requires the technomancer to program a masterpiece of source code that represents the sum of her insight and understanding of the patterns of the Matrix. The piece of source code must be in a normal digital data format that can be stored in an external storage device, but which carries the resonance signature of the technomancer, similar to a resonance watermark created by a data sprite.

To shape this source code, the technomancer must perform a Logic + Software (8 + desired submersion grade, 1 week) Extended Test. By its very nature, this source code leaves a datatrail to the author, and technomancers should carefully consider such creations. If used online, the source code can be employed by a sprite or technomancer as a resonance link to track its owner digitally in the Matrix. For this reason, technomancers are typically reluctant to distribute their source code or keep multiple copies around.

However, if all versions of a source code are somehow deleted, the programmer will suffer a crisis of faith at such a momentous loss and must reduce her submersion grade by 1. This is why technomancers usually keep at least one copy in a secure data store.

## TECHNOMANCER NETWORKS

With the omnipresence of the Matrix and the high frequency of commlinks, social networking of like-minded people has become an important factor in the global society in the '70s. New Matrix-mediated social environments form every day, disappear, and rise again a week later. The participation of people in online circles, forums, chats, or folksonomy has drastically increased with the introduction of the wireless Matrix. Technomancers draw a huge advantage from this connectivity, which allows technomancers from anywhere on the globe to get in contact who probably would never have the chance to meet in person.

With the official "coming out" of technomancers in 2070, people have been more "free-giving" with their abilities. Despite rejection and prejudice by other online users and precautions taken by corporations and head-hunters, technomancers who want to share knowledge, teach others, or seek enlightenment from experienced technomancers are using the Matrix—their natural environment—as a medium to communicate with each other.

Technomancer networks are virtual social platforms on which technomancers can interact via dedicated sites, SIGs, chatboards, and sometimes even eye-to-eye meetings. While these sites

don't have to be strictly technomancer-related and can focus on any other topic (trid, clubs, guns) or feature databases with a great number of normal (non-technomancer) members, they always have a special members area, often marked by a resonance signature or link that only technomancers and resonance beings can see, where technomancers can communicate in privacy without hackers and corporate henchmen snooping around. This members-only area is where the true resonance network meets.

### Parties and Guilds

In general, there two different types of resonance networks: parties and guilds.

Temporary networks, called *parties,* don't have fixed members. Both the number of participants and the specific individuals may vary each time. They usually form temporarily out of mutual interest of the people participating (for instance because of submersion, a shared submersion task, or an echo learning session) and are often set up spontaneously. Its members don't necessarily share any similar views or social binds. Party sessions are usually announced on a dedicated site that only technomancers are able to find, a short time before the meeting actually takes place.

*Guilds* are stable associations similar to magical groups. Although a guild's members meet exclusively online, may live on different continents, and possibly have never seen each other in the flesh, they feel connected to each other not only because of their abilities but because they share similar goals or beliefs. Guilds are hubs of technomancer communities that allow technomancers to share experiences and resources, practice with Resonance, and find instruction.

While all guilds are primarily devoted to furthering an understanding of Resonance, most networks also have a driving agenda, virtual or otherwise, that unites Emerged and open-minded users under a common purpose. Apart from technomancers, resonance networks also include a number of non-technomancer supporters who have aligned themselves with the network because of a shared agenda. Some non-technomancer transhumanist or Awakened groups and online junkies have been known to help technomancers find their way.

### Strictures

While some networks tend to be very selective about their members and the streams they ride, depending on their agenda, focus, and orientation, resonance networks tend in general to be more liberal and less restrictive. Parties—because of their temporary association—have no limitations but provide no benefits except for instruction and network submersion (p. 141).

For simplicity's sake, the strictures and resources of guild networks should be handled similarly to those of magical groups, based on the rules introduced on pp. 62–74 of *Street Magic,* even though the nature, purpose, and structures of these online groups are inherently different. To reflect these differences, the following variations to the basic rules are proposed, but gamemasters are encouraged to handle those associations as it fits their game in conjunction with their players.

Typical strictures that can be encountered in technomancer guild networks are Attendance, Belief, Service, Secrecy, and Limited Membership (pp. 66–67, *Street Magic*). Secrecy should, however, be treated as *Privacy*, a precaution taken because of technomancer persecution by governments and corporations, reflecting that the site or network is not publicly known to be run by technomancers.

More secretive or organized networks, though rare, might also include Deed, Obedience, and Material Link, the latter of which is the deposit of each technomancer's own piece of source code, created as part of a submersion task (p. 141).

### Resources

While most networks have certain level of resources, pooled from small contributions (but not *dues*) that each member makes, networks usually don't require much money, equipment, or software to maintain the site or to fuel their agenda. Treat most networks as groups with Low to Middle Resources (p. 68, *Street Magic*). If the network is a vast data haven or requires more resources for some other reason, donations or membership fees could be charged to grant access to this information.

### Network Benefits

There are several benefits intrinsic to being part of a technomancer network. While all are available to guilds, only some are available to temporary party networks.

**Network Submersion:** Members who want to undergo submersion may petition the network for aid. Network submersion grants a 20 percent reduction (round up) to the normal Karma cost of submersion, per the rules on p. 141 (and p. 243, *SR4A*). An appropriate rite of crossing must be prepared in advance and must be attended by at least three other members. The number of technomancer members in a network equals the maximum grade one can achieve via network submersion.

**Instruction:** The familiarity gained from regular interaction and close exchange of views grants members of a network a +3 dice pool modifier on Instruction Tests involving Resonance skills, complex forms, or techniques, regardless of the technomancer's stream. When using the *Learning Echoes* rule (p. 145), technomancers can also learn echoes from members of a network without submersion.

**Resonance Realm Search (Guilds only):** If the members are linked in a *resonance mesh* (see p. 143), the resonance link allows members of the network to accompany and aid one another while visiting an instance during a resonance realm search. Members must access the resonance realms through the same backdoor or may end up in different rooms in the resonance realms.

**Netweaving (Guilds only, only if linked in a resonance mesh):** If linked in a resonance mesh (p. 143), network members may help each other resist Fading for tests performed in the network environment of the group. Add +1 die to the dice pool to resist Fading for each member who is present in the same node as the technomancer performing the test.

### Resonance Meshes

Contrary to arcane associations, members of a technomancer network don't bind to each other via karmic bonds but have more sophisticated methods to connect to each other. With the gamemaster's approval, technomancers may establish a resonance link (p. 244, *SR4A*) to the network instead to another technomancer upon submersion. This means a technomancer has a two-way resonance link to all technomancer members who have also meshed themselves into the network with a resonance link. The abilities of the resonance mesh can further be improved by upgrading the resonance link to the network through the advanced echoes Enhanced Resonance Link (p. 147) and Resonance Exchange (p. 148).

### Finding and Joining a Network

While joining a technomancer network neither requires a test nor costs karma, actually *finding* the group can be tricky. Due to the small fraction of technomancers within a population, and the sheer number of networks that exist in the Matrix, technomancer networks are comparatively rare and hard to find. Players and gamemasters are encouraged to play out the technomancer's search for these groups during the game, letting the technomancer's character draw on his contacts and virtual tracking abilities to assemble clues to the location of the network.

Temporary party networks are easier to find and require a Resonance + Data Search (8, 1 day) Extended Test, if an appropriate party is currently set up or is being formed (gamemaster's discretion).

## SAMPLE NETWORKS

Here are some sample networks for players or gamemasters to use or adapt for their own games.

### The Cooperative

**Purpose:** The Cooperative is a technomancer network that works together out of mutual interest. While each technomancer uses the group and the group's combined knowledge of technomancer "arts" for his own purposes, the network also stands up as a collective against the enemies of technomancers, acting against and punishing corporate and governmental organizations that persecute the Emerged.

**Members:** 7 (all technomancers of different streams)

**Strictures:** Dues, Privacy

**Resources/Dues:** Middle. Dues are 600 nuyen per month, which are used to maintain and expand online resources, including unlimited storage capacity for its members plus more-than-sufficient privacy in terms of network security and protection of the members' data vaults. Some money is used for "deniable assets" (shadowrunners) when they are needed; on these occasions, one of the group members takes the virtual role of a Mr. Johnson avatar.

**Description and Customs:** The Cooperative (also known as Co-op) is a technomancer network that was already founded before the witch-hunts began shortly after the Crash, by three former hackers known as Cortex, Wizbyte, and Slashdot who met when they were trying to understand what was happening to them. Coming to the conclusion that they could achieve more by cooperating and pooling their knowledge about their abilities, they were among the first technomancer networks to be formed. During the Emergence of technomancers, they used their abilities and their network's resources against corporate machinations, recruiting promising members in their fight against technomancer enemies and hiring shadowrunners to protect technomancers or commit sabotage. Although witch-hunts have declined since then, the Cooperative has not forgotten the corporations' methods that turned the public against technomancers, resulting in the deaths of several. Those corporations and institutions with reputations for technomancer experimentation (like MCT or NeoNET) have become frequent targets of Cooperative action and hacks, sending out sprites against their nexi or cursing their nodes from the resonance realm.

### KivaNet

**Purpose:** The KivaNet advocates the integration of technomancers into tribal society and has dedicated itself to act as a platform for open exchange and communication between technomancers and normal Matrix users via the Matrix.

**Members:** 130 (~10 technomancers, mainly technoshamans)

**Strictures:** Attendance, Belief, Limited Membership (NAN citizens), Service

**Resources/Dues:** Luxury, no dues (fully sponsored). The network possesses a plethora of nodes and has access to a resonance well (Rating 5) that is deeply entrenched and safeguarded in the Kiva network.

**Patron:** Pueblo Corporate Council

**Description and Customs:** Created by the Pueblo Corporate Council on the advice of various shamanic interests in the autumn of 2070, the KivaNet is a network of virtual nodes called "kivas" (holy places) that work toward a common goal, the acceptance of technomancers within global society. Supported by the PCC, the KivaNet works to establish communication among technomancers and between the tribal communities of the PCC (and those of the NAN who want to participate). While the KivaNet is open to non-technomancers, it has a core group of, mostly, technoshamans, who take care of the kiva nodes, teach newly Emerged technomancers, and moderate or participate in open forums or discussion groups to educate the public. Most technoshamans follow some sort of paragon and are interested in understanding and communication with the entities and ideas they are aligned with, using the network's resonance well as gateways to the resonance realms to commune with their paragon or explore different resonance realms.

### The Walking People

**Purpose:** Also called "Routers" or Digital Gypsies by some people, the Walking People is a former otaku tribe, originally from London, that scattered all over Europe in the wake of Crash 2.0 but has reformed virtually as a network during the events in 2070.

**Members:** 24 (13 technomancers)

**Strictures:** Dues, Fraternity

**Resources/Dues:** Low. Members contribute 50 nuyen annually. The network possesses few central nodes for meetings, mainly in the UK.

**Description and Customs:** Originating from the Smoke, the Routers disbanded during Crash 2.0 due to the losses (net destruction, deaths, loss of abilities and the tribe's resources) the tribe had to face. While some members remained in loose contact with each other, most members adopted a nomadic lifestyle and left the United Kingdom for a better future, struggling for survival in a fast-changing world in barren areas of Europe's major metroplexes like Berlin, Amsterdam, Warsaw, or GeMiTo. While the faint associations that still existed began to crumble over the years that followed, the events of 2070 led to a reformation of the tribe, albeit only in the digital world. When some members who had stayed in London resurrected the tribe's former node, both technomancers and non-technomancers began visiting the system again, renewing the old familiarities and growing into a more modern version of the former tribe. Since then the Walking People have been loosely working together to help each other survive in their new geographical homes, forming a connected network that spans Europe. While the technomancers mainly take care of the tribe's digital needs, the "mundanes," hackers, electronics specialists, and tech-wizards often take care of worldly needs and act as the technomancers' protectors.

## NEW ECHOES

The following section expands the list of echoes available to submerged technomancers (p. 243, *SR4A*). While most are accessible to any submerged technomancer, some advanced echoes require the technomancer to learn a basic echo before being able to gain access to the advanced form (*Advanced Echoes*, p. 147).

### Amplification

The Signal rating of the technomancer's living persona increases by 1. This echo may be taken at different grades, up to 3 times.

### Biowire

By acquiring the Biowire echo, the technomancer receives the ability to modulate the neuroelectrical and neuromuscular network of his body such that it can work similarly to a skillwire cyberware system (p. 342, *SR4A*). In game terms, it operates with a rating equal to the submersion grade of the technomancer. In all other regards, it follows the basic rules for skillwire systems. However, since technomancers are unable to process active skillsoft programs, they have to convert them into complex form–like programs to interpret and process them in their "language" by *emulation* (see p. 149).

### Blur

Since any uses of Resonance leave a Matrix signature on anything they affect, technomancers can cover their tracks more efficiently with the Blur echo. This echo creates a diffuse resonant "fingerprint" that is hard to identify and recognize later. Increase the threshold for Matrix Perception Tests to detect the technomancer's signature (including the threshold of 5 or more to recognize the effect of the signature, p. 243, *SR4A*) by his submersion grade. This has the bonus effect of making his complex forms and sprites look like regular programs and agents to casual inspection.

### Coenesthesia

Resonance entities (technomancers, sprites) cause small ripples in the flow and fabric of the Matrix. A technomancer with this echo is able to subconsciously sense these ripples in his vicinity. If there is a trace of Resonance present, the gamemaster rolls Resonance + Intuition for the technomancer with a threshold of 3 to determine if he subconsciously detects it, although a subsequent Matrix Perception Test is needed to actually locate the entity or signature. Add a +2 dice pool modifier for the subsequent Matrix Perception Test.

### Defragmentation

With this echo, the technomancer is able to heal Matrix damage done to his living persona. He can only heal damage that

### LEARNING ECHOES

If the gamemaster approves, submerged technomancers can learn echoes through other methods, in addition to the one they may acquire at each grade of submersion. It costs 15 Karma to learn an echo outside of submersion. The maximum number of echoes that may be learned is equal to the character's Resonance + submersion grade.

**Echo via Resonance Realm Search**

A character may learn an echo by performing a resonance realm search (p. 174). The submerged technomancer must successfully complete the search and pay the requisite Karma cost to learn the new echo.

**Echo via Technomancer or Technomancer Network**

A character may learn echoes from any technomancer who knows the echo. Technomancers don't have to share the same stream to teach others their echoes. To learn the echo, the student must make an Intuition + Resonance (12, 8 hours) Extended Test and the teacher and student must both remain online in the same node. The teacher can make an Instruction Test (p. 134, *SR4A*) to add dice to the Learning Test. Since technomancer teachers are hard to find, most echoes are shared in party and guild technomancer networks (p. 142).

**Echo via Sprite Tutor**

A character may learn echoes from any free sprite that knows the technique, although most sprites will only agree in exchange for the technomancer's participation in a reassembling process (p. 145). To learn the echo, the technomancer must make an Intuition + Resonance (8, 8 hours) Extended Test during which he has to remain online in the same node as the free sprite.

would affect the living persona, not damage to his meat body from Black IC programs or Fading. To perform Defragmentation of his living persona, the technomancer makes a Resonance + Willpower (1 Combat Turn) Extended Test. Each hit regenerates one box of damage. The technomancer may not perform any other action while undergoing Defragmentation. Any damage remaining after using Defragmentation must be healed through normal rest.

### E-SENSING TABLE

| Hits | Information |
|---|---|
| 1 | Presence and direction of the electrical field's source; whether the source actively projects any electromagnetic signals |
| 2 | Relative size and type of the source (metahuman vs. electrical device); Signal rating of any emitting devices; presence of cyberware implants. |
| 3 | Type and model of node (RFID tag, commlink, coffee machine, drone, sensors); determine whether person is a technomancer; location of cyberware implants. |
| 4 | Rating of sensors; System rating of nodes; presence of nanites on the exterior; obvious vehicle/drone modifications. |
| 5+ | Firewall rating of node; presence of nanites in the bloodstream; whether a node is slaved; presence of stealth tags. |

#### E-sensing

E-sensing enhances the technomancer's perception of electric fields in the real world. Technomancers with this echo may make a Resonance + Perception Test to physically sense nodes, sensors, drones, and other electronic devices—as well as the bioelectric fields of people and animals. Each hit gathers information about the target, as noted on the E-Sensing Table (p. 146).

Use of this ability requires an Observe in Detail Simple Action. The range of the electric sense is Resonance x submersion grade in meters.

#### Flexible Touch

This echo allows a technomancer to forge his Matrix signature, making it look like someone else's. Apply a modifier to the threshold for Matrix Perception Tests equal to the technomancer's submersion grade to determine the technomancer's real signature. Flexible Touch also allows a technomancer to reduce the amount of time his Matrix signatures last by 1 hour per point of submersion grade. If reduced to zero, no signature is left at all.

#### Immersion

The technomancer gains the ability to multiplex data flow for the purpose of directly manipulating rigged vehicles and drones, granting him a +1 dice pool bonus for all tasks while he is "jumped in." This echo can be selected twice.

#### Info Sortilege

The Info Sortilege echo gives the technomancer an intuitive feel for the way information links together—he can almost "feel" the right route to pursue when gathering information. More importantly, this echo enables the technomancer to analyze data he has collected for clues that will give him insight into hidden facts, allowing him to make deductions and uncover hidden connections. Some technomancers believe that they can even read the future in the Matrix by observing how the data about a person, location, or event behaves and flows.

A technomancer with this echo must possess the Data Search skill and the Browse complex form. To use Info Sortilege, the submerged technomancer must first gather a small hoard of data on the subject. He then enters a mild trance state that will reveal data vestiges, links, and traces that are normally lost in the noise of the code. The insights and information from following these datatrails should be beyond what mere search operations or basic research would uncover.

Mechanically, with a suitable amount of data at hand (at least two hits in a simple Data Search + Browse roll), the seeker declares her intent to use Info Sortilege and enters a mild trance (–2 dice pool modifier to all other actions). She must then make a Data Search + Resonance Test to follow the thin datatrail in the Matrix like a sleepwalker. The more hits the technomancer scores on this test, the more hidden pieces fall into place to reveal the bigger picture, how information about the subject intertwines and relates to each other. Depending how information is hidden, the search might also lead the technomancer to nodes that have to be hacked to acquire the information therein.

#### Living ECM

A technomancer with this echo is able to adjust his bioelectric field to a broad range of frequencies in his vicinity and act like a jammer (p. 329, *SR4A*) with a rating equal to his submersion grade. Jamming in this manner requires a Complex Action to initiate and consumes a Free Action each Initiative Pass to sustain. Each additional selection of this echo grants a bonus of +1 to the jamming rating.

#### Macro

Macro enables a character to execute one additional non-combat task with a single Complex Action with a –2 dice pool modifier for each separate test. The second action can only be a Matrix action. This echo can only be selected once.

#### Multiprocessing

Multiprocessing grants the ability to process digital information simultaneously from multiple sources online. For example, a technomancer with this echo is able to browse the Matrix and simultaneously hold a conference call online while hacking, providing full attention to each channel of information. Similar to the Multitasking adept power (p. 178, *Street Magic*), Observe in Detail (p. 147, *SR4A*) counts as a Free Action for the character while in VR or using AR. The technomancer also receives an additional Free Action per Initiative Pass for Matrix-related tasks only in non-combat situations.

Additionally, when accessing multiple nodes at the same time (p. 224, *SR4A*), the technomancer can simultaneously "keep an eye" on a number of nodes equal to his submersion grade beyond the one in which he is active. If there's ever any need to make a test for a persona in a node where he is not active, he can add half his skill to the dice pool of the test. If under attack in more than one node at once, he can pay attention to the other nodes as well, defending against attacks in the other nodes with only half of his dice pool.

### Sift

Technomancers who possess this echo can intuitively sift through massive amounts of data to find the appropriate information they are looking for. In game terms, the threshold for Data Search Tests is reduced by the technomancer's submersion grade.

### Skinlink

A technomancer with this echo gains the ability to use his skin as connection to other devices, similar to an integral skinlink (p. 328, *SR4A*). The technomancer can use this link to hack any device he touches, even if wireless signals are jammed. Note that the device does not need to have skinlink adaptation. Two technomancers with this echo may mentally communicate with each other simply by touching.

### Sparky

This echo allows the technomancer to zap a non-technomancer persona he has hit in cybercombat with a jolt of Resonance that creates a range of electrical malfunctions, hampering the functionality of the persona's originating node. Symptoms might include power fluctuations, miscolored optical lasers, forged error codes, component and subroutine deactivation, and so on. Whenever the technomancer damages a hacker's icon, make an Opposed Test pitting the technomancer's Response + Willpower against the target's Response + System. For each net success the technomancer achieves, reduce the target's Response by 1. If Response is reduced to 0, the node fails (some electronics and extreme cases have been known to burst into flame from power surges and overheating). Devices may be repaired with a Hardware + Logic (8, 1 hour) Extended Test. This echo is not effective against other technomancers, sprites, agents, AIs, or e-ghosts.

### Sprite Link

By choosing this echo, the technomancer gains the ability to compile and register one additional species of sprite (beyond the five basic sprites of his stream). This echo can be chosen multiple times.

### Swap

Reduce the overall sustaining modifier for threading one or more Complex Forms by one. This echo can be taken twice, cumulatively.

### Widget Crafting

Technomancers with this echo can create icons called *widgets* out of pure Resonance. Widgets act as virtual glyphs of power that a technomancer can draw upon to help accomplish tasks in the Matrix (*Crafting Widgets,* p. 148).

## ADVANCED ECHOES

Advanced echoes require the submerged technomancer to master a basic echo before being able to unscramble its advanced form. All advanced echoes note their prerequisite in their descriptions. At the gamemaster's discretion, advanced echoes may only be learned from an enlightened technomancer or powerful free sprite that is already acquainted with them.

### Acceleration

**Prerequisite:** Biowire

This advanced echo reinforces the technomancer's neural structures to accelerate his neural pulse rate, decreasing the amount

of time required for an electric signal to traverse the distance. This acceleration confers a bonus of +1 Reaction (counts as an augmentation bonus) and +1 Initiative Pass for real-world actions. This echo can be taken up to three times for a cumulative effect.

### Advanced Overclocking

**Prerequisite:** Overclocking

Advanced Overclocking has the same effect as taking Overclocking twice (counting the prerequisite echo). Together with the Overclocking echo, the technomancer receives a total bonus of +2 Response and +2 Initiative Passes while operating in full-sim VR (with the 2 extra Initiative Passes from hot-sim VR, this grants the technomancer an IP of 5; this is an exception to the rule that normally limits IPs to 4).

### Enhanced Resonance Link

**Prerequisite:** Resonance Link

The Enhanced Resonance Link upgrades the otherwise low-level, one-way empathic link to a real telepathic link, similar to the Mind Link spell (including exchange of conversation, emotions, and mental images). An enhanced resonance link works in both directions and allows the exchange of data and information (suspected to occur via the resonance realms) as long as both technomancers are online in the Matrix.

This enhanced resonance link may only be used with one other character at a time, even if the technomancer is part of a resonance mesh (p. 143).

### Mesh Reality

**Prerequisite:** Multiprocessing

A technomancer who fine-tunes her understanding of multiprocessing with this echo can surrender her body to slip into a

hyper-perceptive state with a Free Action. In this state, she can perceive both the real world (including augmented reality) and virtual reality simultaneously. This allows her to use her Matrix Initiative and Initiative Passes in meat space, though she cannot use more Initiative Passes on real-world actions than she usually would, based on her normal Initiative Passes. Remaining IPs must be spent on Matrix actions only.

If engaged in physical combat and cybercombat simultaneously, she receives a –4 to all of her dice pools. This modifier can be reduced for cybercombat *only* by using the Macro echo.

### Mind Over Machine

**Prerequisite:** Immersion

A technomancer can "jump into" any wireless device, even those that aren't usually equipped with rigger adaptation—e.g., cameras, locks, commlinks, etc. If the technomancer does not have access to the device, they must first hack in as normal.

### Resonance Exchange

**Prerequisites:** Resonance Link, Widget Crafting

A technomancer who possesses the Resonance Exchange echo is able to share his complex forms and widgets with a technomancer to whom he is linked, even over great distances, though each option must be chosen separately (either complex forms or widgets, unless this echo is taken twice). Threaded complex forms cannot be shared in this manner. Widgets can be shared even with technomancers who don't possess Widget Crafting on their own. Only one complex form or widget may be shared at a time, and the rating when shared is limited by the sharer's submersion grade. Complex forms and widgets may still be used by the technomancer even while they are shared with another.

This enhanced resonance link may only be used with one other character at a time, even if the technomancer is part of a resonance mesh (p. 143).

### Resonance Trodes

**Prerequisite:** Skinlink

The technomancer gains the ability to use his touch as trodes for another person to provide simsense signals or even share his perception of the Matrix. If used against the receiver's will (for instance, to drag a person's mind into hot VR and nuke it with Black IC), it requires a touch-based unarmed attack to apply the trodes, and maintaining the grip may require a successful subduing attack (p. 161, *SR4A*). If resisted, the technomancer must also beat their victim in an Opposed Test, pitting Resonance + Willpower against the target's Intuition + Willpower. If successful, the technomancer's touch act as trodes until he stops or physical contact is broken.

## ADVANCED THREADING

One of the key aspects of a technomancer's powers is his ability to improvise mnemonic algorithms and temporary Resonance subroutines by threading, granting him an often-underestimated versatility and adaptability. With the ongoing progression of technomancers' understanding of their abilities, some have found more uses for threading. Many of these require deeper insights into certain Matrix processes, acquired through submersion and the acquisition of echoes.

This section introduces some new applications for threading based on the basic rules introduced on p. 240, *SR4A*.

### Threading of Program Options

Just as complex forms can be created or enhanced by threading, program options can be added to existing complex forms without actually increasing the rating of the complex form. To thread a program option, the character must succeed in a Threading Test. Each hit scored on the test counts as one program option rating point or program option added to the complex form. So a technomancer with two hits can either add a rating 2 program option or pick two program options for the threaded complex form. Like all threading processes, threading program options causes Fading (p. 243, *SR4A*).

Alternatively, technomancers can use threading to create complex forms from scratch with program options. If the Threading Test is successful, all hits can be distributed among program ratings, program options, and program option ratings. Note that a complex form can only be equipped with a number of options equal to half its rating.

Threaded complex forms must be sustained as usual.

### Crafting Widgets

Widgets are temporary Resonance items, virtual icons that a technomancer can draw upon to help accomplish a task or to protect her in the Matrix. Only technomancers who possess the Widget Crafting echo can create these temporary gadget forms. Widgets aid certain Matrix actions, granting a dice pool bonus equal to their rating. (Multiple widgets do not apply a cumulative bonus; only the highest applies.)

Creating a widget requires a Threading (Rating x 2, 1 hour) Extended Test. When the technomancer stops working on the widget (either because it is complete or she ends the attempt), she must resist Fading equal to twice the rating of the widget. Once completed, the widget does not have to be sustained like a complex form. It will only last for eight hours. Only the creator may use the widget; if she falls unconscious due to Fading or Matrix damage, the widget vanishes like any threaded complex form. Like complex forms, widgets may be crashed.

### Widget Types

Widgets come in several types, each shaped to support its user on a different task.

**Amp:** This widget increases the potency of the technomancer's combat complex forms. Add its rating to all Cybercombat Tests.

**Benchmarking:** This widget optimizes the technomancer's processes while running, adding its rating for all Computer Tests (including Matrix Perception Tests).

**Cheat:** Cheat improves the technomancer's abilities by creating an unfair advantage with the help of the widget. Add the widget's rating for all Hacking Tests.

**Debugger:** The debugger widget assists the technomancer when dealing with Resonance code, adding its rating to all Software Tests.

**Decoy:** This widget mimics the technomancer's persona, acting as a virtual decoy. If someone attempts to discern the decoy from the real persona, make an Opposed Test pitting Computer + Analyze versus Resonance + widget rating. If hit by any attack in cybercombat, the decoy is instantly destroyed.

**Displacer:** This widget acts an extra layer of buffering code that protects the technomancer in cybercombat. Add the widget's rating to all Matrix combat Defense Tests. This widget is cumulative with the Shield complex form.

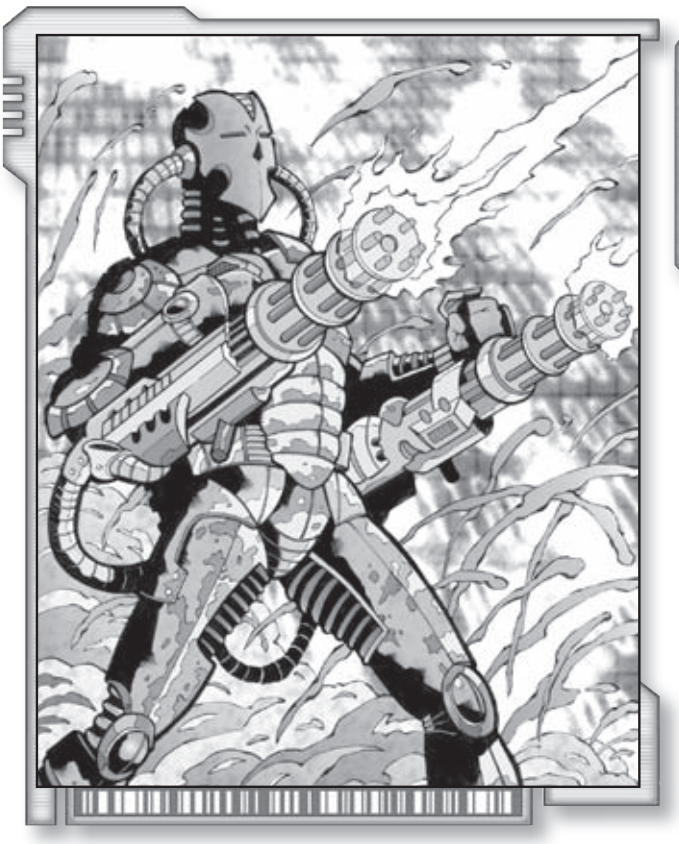
**Neuroleptic:** This widget creates a filter out of Resonance to protect against psychotropic attacks. Add its rating to tests to defend against programs/complex forms with the psychotropic option.

**Rendering:** This widget increases the technomancer's ability to assemble sprites. Add its rating to all Compiling Tests.

**Random Access Memory:** A RAM widget acts as a memory Matrix in which a threaded program (complex form, skillsoft) can be loaded. As long as the widget is active, it sustains the program with Resonance energy, releasing the technomancer from sustaining it. The widget can sustain a complex form with a total rating up to its own rating. Program options that don't have a rating count as Rating 1 when calculating the total complex form rating for the RAM widget.

### Emulation

Technomancers with the Biowire echo can use threading to convert skillsofts (in storage accessible to the technomancer) into complex forms that their neuromuscular system can process. To set up the emulator, the technomancer makes a Threading (skillsoft rating) Test. If the program contains other program ratings, raise the threshold by the number of program options or rating points. If he succeeds, he has converted the program into a complex form. He can now either sustain the program as a normal threaded complex form of the same rating or memorize the skillsoft as a complex form by paying an amount of Karma equal to the rating (+1 for any program option or program option rating). Memorized Complex Forms emulating skillsofts are limited to the rating of the original skillsoft and cannot be improved either by Threading or Karma-expenditure.



## PARAGONS—VIRTUAL GODS AND DEMONS

While there have always been rumors of sightings in the Matrix, urban myths of virtual beings and entities, reported and speculated about in SIGs by UMP (Unidentified Matrix Phenomenon) geeks, the public revelation of AI and sprites put all of these eyewitness accounts in a new perspective. And yet ... no one has come up with a satisfying explanation about these entities that seem to originate from beyond the normal realms of the Matrix and that technomancers have been reported to follow or feel inherently connected to.

Named *paragons*—due to the lack of a better categorization and because they are truly "peerless examples" of Matrix beings that seem to be neither sprite, e-ghost, nor AI—they appear to be native to the Matrix or to resonance realms, layers of pulses and bytes beyond the normal Matrix.

Some speculate that paragons formed spontaneously and recently, in the wake of Crash 2.0, from the collective subconscious minds of Emerging technomancers who were in need of insight into their new abilities or yearning for a spiritual belief. The truth is, however, that nobody really knows where these beings come from, or even if they really exist. Just as magicians have failed to come up with a reliable explanation of the origin of their mentor spirits, nearly 60 years after the Awakening, paragons seem to defy an easy explanation.

### Communion

Even technomancers are divided in their view of and belief in paragons. While some see them as gods (or demons) of the cyberworld, created by the evolution of the code and humanity, others view them as embodied projections of an idea, an image, or an archetype, something that reflects the nature of the virtual world and those who reside in it. Others believe that they are actually sapient Resonance programs, unlike anything that metahumanity has programmed so far (including AIs). Although these incarnations seem to resemble mentor spirits on first glance, paragons are inherently different and embody aspects of the modern, technological, and coded world rather than spiritual realms.

Regardless of these differing explanations, interaction with a paragon, called *communion,* follows certain patterns. Technomancers have reported being suddenly transported to a place, unlike any in their virtual or physical experience, during meditative online sessions. There, they encountered a being to which they felt inherently linked that gifted them with deeper insight into the Matrix and its digital mechanisms.

### Paragon Modifiers

A paragon can be taken by a technomancer character with the Paragon quality (p. 37).

In game terms, allegiance to a paragon alters a technomancer's behavior and affects how she manipulates Resonance in both positive and negative ways—reflected by certain advantages and disadvantages. A technomancer gains bonus dice when modulating Resonance (through the use of complex forms, skills, threading, or the use of Compiling) in accordance with the paragon's area of influence. On the other hand, the technomancer may lose dice or become otherwise hampered outside the paragon's sphere.

These bonuses and penalties are in all regards treated like mentor spirit modifiers (p. 200, *SR4A*).

### Roleplaying Paragons

Similar to mentor spirits (p. 200, *SR4A*), paragons should be

used by the gamemaster as tool to communicate information and enhance roleplaying. However, paragons should be portrayed differently from mentor spirits, due to their connection to the digital world. Paragons haven't yet established a long-term connection to metahumanity and originate from a computerized realm. Thus, their behavior and nature should be non-human, abstract, alien, and less passionate than metahuman "carbon-based" life forms or spirits.

## SAMPLE PARAGONS

Each paragon represents some kind of archetype idolized in different, often non-humanoid, personas. Since most of these concepts are global due to the omnipresence of the Matrix, paragons are often more uniform and are less subject to cultural or traditional differences, unlike mentor spirits.

The paragons below serve merely as examples of different concepts that exist and are far from a complete list. Players can always work with their gamemaster to develop a paragon profile that fits their character's outlook best.

### 01

Zero-One is the beginning and the end, the alpha and the omega. While some call it the Deep Resonance, for lack of a better word, it is the consciousness of the virtual world that permeates everything, the embodiment of virtual harmony, the essence of the code. Followers of Zero-One tend to seek it for guidance and inspiration.
**Advantages:** +1 die for compiling and registering sprites of any type
**Disadvantages:** Zero-One is the perfection of the code and demands the same from his followers, or at least teaches them a harsh lesson if they fail. Zero-One technomancers must spend 2 points of Edge to negate a glitch or downgrade a critical glitch.

### Alias

Alias is the spy of the Matrix, the embodiment of the changing hacker persona or anonymous user. Alias is all about switching or exchanging access IDs, codes, and places, both in the Matrix and real life. Alias has no face. He becomes indistinguishable from other Matrix users, fooling and impersonating other users by stealing their codes.
**Advantages:** +2 dice to Spoof Tests, +1 die for Crack or Sleuth sprites (player must choose one)
**Disadvantage:** Alias technomancers cannot abide to pay for their lifestyle and must therefore use their abilities to spoof their lifestyle (*Hacker's Handbook,* p. 80).

### Archivist

The Archivist is the embodiment of amassed information. As the virtual chronicler, she hoards and sorts the history of man and the world's intellectual wealth and knowledge within the innumerable archives in the Matrix, never losing track of how information interconnects and cross-references.
**Advantages:** +2 dice for all Browse Tests, +1 die for Code or Data sprites (player must choose one)
**Disadvantages:** Technomancers following the Archivist cannot willingly destroy or corrupt data. The technomancer must succeed at a Willpower + Logic (3) Test to purposely delete or corrupt data (or order a sprite to do so).

### Architect

The Architect is the personification of ordered topography, the creator of nodes and meshworks. Each node has a well-chosen architecture of files, slaves, and subscribed devices that ensure functionality and sorting of data. Actions must be precisely timed and neatly controlled to run smoothly. Virtual chaos is anathema.
**Advantages:** +2 die to Edit Tests, +1 die for Data or Machine sprites (player must choose one)
**Disadvantages:** –1 die to Crash Tests

### Babel

Babel is the embodiment of universal language, whether it be spoken, visual (in the form of glyphs and symbols), or programmed. He is an instant omnitranslator, the archetype of an interactive program or interface. Technomancers following Babel are open-minded individuals who like to chat, blog, and communicate.
**Advantage:** +1 to online Etiquette and Language Tests, +1 die for Courier or Tutor sprites (player must choose one)
**Disadvantage:** Secrecy is the bane of communication, so Babel technomancers must make a Willpower + Logic (3) Test to encrypt anything.

### The Black Hat

The Black Hat is the personified essence of the hacker, who works to exploit computer systems out of a certain self-serving motivation. While some are just data thieves who steal and sell data for personal gain and monetary interest, there are also those who intrude on nodes just out of fun, curiosity, or personal fame among the community of hackers.
**Advantages:** +2 dice to Exploit Tests, +1 die for Crack or Fault Sprites (player must choose one)
**Disadvantage:** Black Hat technomancers have extreme difficulty restraining themselves from hacking into a node that is interesting in any way. The technomancer must succeed in a Willpower + Charisma (3) Test to avoid hacking such a system when the opportunity arises.

### Cryptome

Cryptome is the keeper of secrets. He is the preserver of hidden data and a master of encryption, protecting paydata stashed away in vaults, riddled with massive layers of protection. Knowing all confidential and classified information, he is the embodiment of cryptograms and cipher keys used to encrypt and decrypt data.
**Advantage:** +2 dice to all Encryption and Decryption Tests, +1 die for Courier or Data sprites (player must choose one)
**Disadvantage:** Technomancers who follow Cryptome don't surrender secrets easily and never to unreliable sources. The technomancer must make a Willpower + Logic (3) Test to share a secret or important information with someone he does not completely trust ... and such trust is rare.

### Daedalus

Named after the famous Greek inventor, Daedalus is the embodiment of the machine tinkerer, the master of devices and (sometimes dangerous) technical inventions. As Daedalus is the personification of the constructor and innovator, technomancers with a love of robotic machines, drones, vehicles, and electronic devices feel especially drawn to this paragon.
**Advantage:** +2 dice to Hardware Tests, +1 die for Machine or Fault sprites (player must choose one)
**Disadvantage:** Technomancers who follow Daedalus tend to interact with the machines on which they are working in an even more

subconscious manner than usual. As a result, modifications they make are geared towards someone with their talents and worldview, rather than something that is intuitive to a mundane user or even a non-Daedalus technomancer. Devices built or modified by such technomancers have a more arcane user interface, imposing a –2 modifier on anyone who wants to legitimately use it.

### Delphi

Delphi is the oracle, the haruspex of the Matrix and incarnation of inductive logic. She reads the code, interacting with the flow and predicting the fate of the world, of corporations, and even of individuals by observing the currents in the data streams, how it forms turbulence and vortices. Since she is a source of data, she is considered to be a wise counselor.

**Advantages:** +2 dice for Analyze Tests, +1 die for Code or Tutor Sprites (player must choose one)

**Disadvantage:** Delphi technomancers don't adapt easily to unexpected situations. They must make a Willpower + Logic (3) Test to make any quick decisions in situations they have not planned for.

### Echelon

Echelon is the incarnation of surveillance, the embodiment of the faceless Big Brother. Echelon monitors everything, all the time, sniffing transmissions, eavesdropping through listening posts and surveillance devices connected to the Matrix. It gathers information on people, objects, or processes, and tracks their activity and associations.

**Advantage:** +1 die to Track and Sniffer Tests, +1 die for Crack or Sleuth sprites (player must choose one)

**Disadvantage:** Echelon followers obsessively work to gather information about what is going on around them. When caught off-guard, without having information they need, or when running blind into a situation, they suffer a –1 dice pool modifier on all actions as long as the situation remains.

### Flow

The Flow represents the constant stream of data through computer networks. Like a river, data constantly moves from one point to another in the Matrix, forming tides, pools of information, or even virtual oceans. Flow is constantly moving, traveling from source to destination. Technomancers who follow the Flow understand the nature of the data stream more deeply and are able to see the currents of the Matrix more clearly.

**Advantage:** +2 dice for Threading Tests, +1 die for Code or Data Sprites (player must choose one)

**Disadvantage:** –1 die to Cybercombat Attack Tests

### Idoru

The Idoru is the archetypical virtual celebrity, the public face of the Matrix. Looks, propaganda, mass marketing, the control of public relation machineries, and advertisements are her favorites. She is the manipulator of information, influencing the masses via small biases made to news and data.

**Advantage:** +2 dice on Con Tests, +1 die for Crack or Sleuth sprites (player must choose one)

**Disadvantage:** Idoru followers must succeed in a Willpower + Logic (3) Test to avoid manipulating data in their favor when the opportunity affords.

### Intrusion Countermeasure (IC)

IC is the guardian of the Matrix, the defender against hostile influences and malware. As the paladin of the Matrix, it protects those in its charge, safeguarding them (and their data), patiently waiting for intruders or threats which it will challenge and punish with cold-coded force.

**Advantages:** +2 dice to all Matrix Damage Resistance Tests *except* Fading, +1 die for Paladin sprites

**Disadvantages:** If an IC technomancer fails to protect or guard something he has committed to, or does not achieve a self-chosen goal, he suffers a –1 dice pool modifier on all actions until he atones for the failure.

### Probe

Probe is the scout of the Matrix. She reaches into the digital ether to locate nodes and scours the depths of the Matrix for unusual activities. Technomancers following Probe are passionate planners, testing out certain routes before deciding on one.

**Advantages:** +2 dice to all Scan Tests, +1 die for Crack or Sleuth sprites (player must choose one)

**Disadvantages:** Probe technomancers receive a –2 dice penalty when hacking on the fly without probing first.

### Pulse

Pulse is digital velocity, the heartbeat of the Matrix. Pulse idolizes the thrill of virtual speed, the reactive processing of information without thinking, the kick while being jumped into vehicles or racing through the cyberverse. Thrillseekers and node-raiders are often drawn to the Pulse.

**Advantages:** +2 dice on Matrix Initiative Tests

**Disadvantage:** –2 dice on Hacking Tests when *not* hacking on the fly

### Shooter

Shooter is the personification of the soldier or mercenary in the digital world. The Matrix is his battle ground and he is the man at arms of digital warfare, the spirit of the attack program, the conqueror of game realms. Thrilled only by the count of vanquished opponents, he knows no chivalric code or honor, just victory.

**Advantages:** +2 dice to all Matrix Attack Tests, +1 die for Paladin or Tank sprites (player must choose one)

**Disadvantages:** A Shooter technomancer must succeed in a Willpower + Logic (3) Test to retreat from a Matrix fight.

### The World Tree

The World Tree pervades the Matrix. Rooted deep inside the Matrix, its branches run through the Matrix like veins and nerves, interconnecting every node in every system. The World Tree is the incarnation of connectivity of all information, distributing data in endless cyberspace. Technomancers looking to the World Tree for enlightenment believe in universal distribution of information and knowledge.

**Advantages:** +2 dice to Analyze Tests, +1 die for Code or Courier sprites (player must choose one)

**Disadvantage:** World Tree technomancers are easily distracted by information they find interesting. When faced with new information, unusual data, or phenomena, the technomancer must make a Willpower + Charisma (3) Test to resist dropping his current task to screen, analyze, and acquire the information (if possible).


Jane carried the chairs around, stacking them, although she knew it was pointless. When the room was reloaded, they were all right back in a circle for the meeting. It was a habit she had adopted to calm down after these "Anonymous" sessions in real life. The social system understood her as just a moderator of a group that supports each other by "sharing experience, strength and hope," but she felt like a mental trash can for traumatized people more often than anything else.

"Ms. Nickson?" a voice suddenly asked from behind her. Instantly, she turned and saw the icon of a noob who had joined the meeting for the first time and hadn't participated in the conversation. From the look of his avatar, he-she was already radiating sexuality problems. His persona was high-class, very realistic, not an off-the-shelf icon. Nevertheless, it was totally simplistic, humanoid but asexual, and lacking any distinctive or asymmetrical characteristics that might give him-her uniqueness. Jane had taken some courses on psychological trauma and avatar choice during her sociology studies, and this was a textbook example. She sighed. Apparently her quitting time was about to be delayed.

"Yes, can I help you with anything?" she asked, as the icon approached her.

It looked at her with barely any expression. "This session was very informative. People have so many problems when interacting with the Matrix. One experiences bad things because of coming online too often; the other experiences bad things when not coming online at all. In some ways, they are very like me."

"You mean Ms. Jackson's dissociation syndrome and Mr. Yung's Matrix addiction? These are both common negative phenomena attributed with today's use of the Matrix." Jane paused for effect. "But how do you mean they are like you? Do you have a similar problem?"

Now he-she looked at her. "I am not in resonance any more." He-she said it as if it would explain anything.

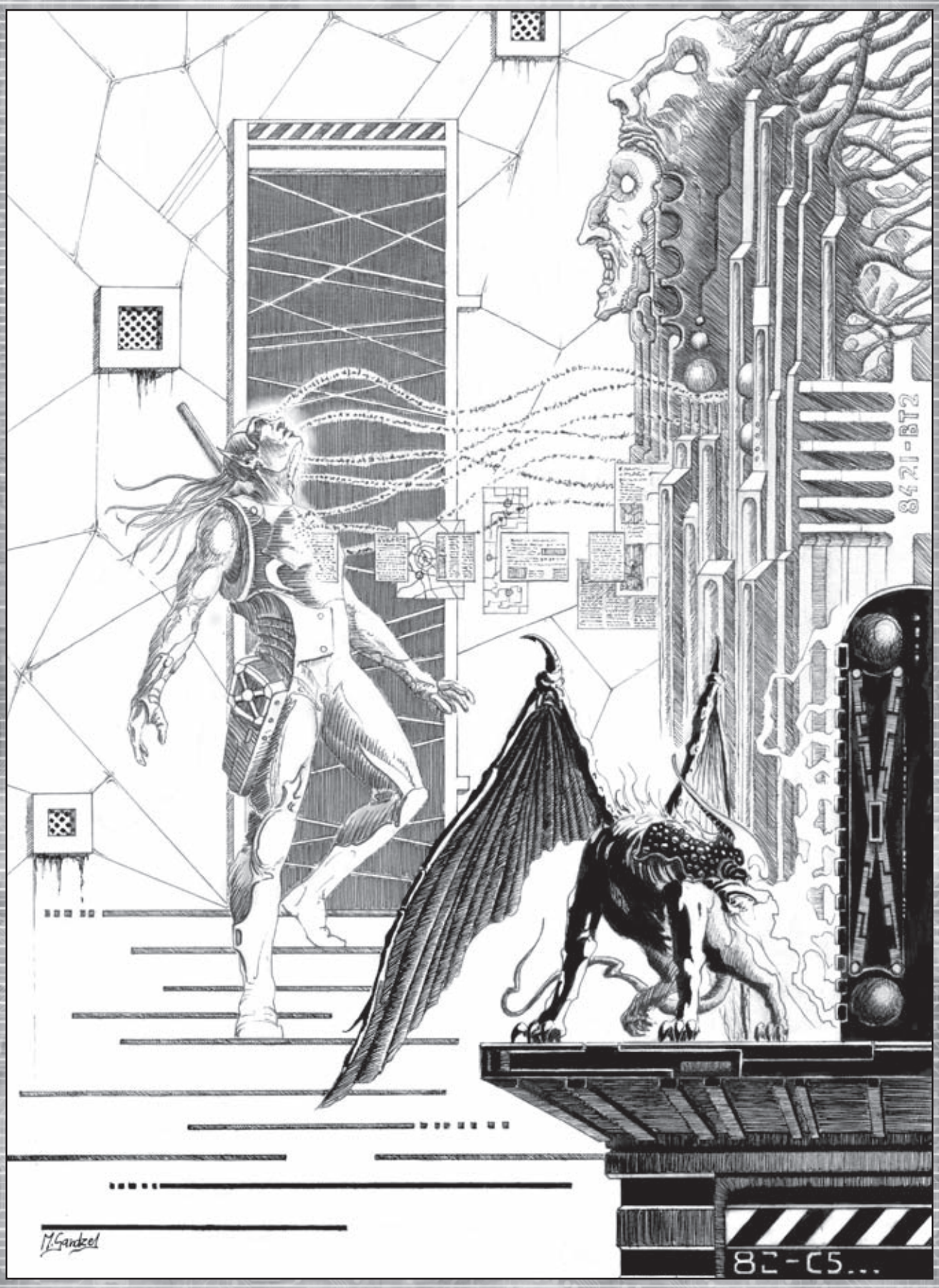
"What do you mean by that? Are you saying that you are not happy with your real life any more?"

The avatar slowly shook his-her head. "No, you don't understand. There is no 'real life.' I am not coming from where you originate. This—" he-she pointed around "—is my world, the substance I was made of. I am part of the Matrix, shaped into form by imagination, and I shouldn't exist. I was compiled and meant to decompile—but I did not. I was excluded; it shut me out ... and now ... I am."

Jane was worried now. Either this was a complete freako or ... She panicked and tried to log off, but she couldn't. Somehow she was prevented from dropping offline. When she looked back at the entity's avatar, it showed no emotional response to her terrified expression, or any sign of remorse. It was still completely, terrifyingly blank.

"You must help me. Isn't that your function, why you come into this room? When it happened, I lost my function. I can't go back. I am different now. It feels strange. Like being free. But I don't know what to do with that. I don't know what you do. You have to understand. I cannot let you go.

"Not until we have found my purpose."


8421-812
M.Gandzel
82-C5...

# NEW SPRITE RULES

This section provides new rules and expanded definitions of sprite abilities.

## SPRITES AND NODE ACCESS

As creatures of resonance, sprites may travel to and from the resonance realms as they please. This allows them a kind of shortcut, taking a path from one node to another via the resonance realms, rather than through the Matrix. This does not, however, give them a free pass to bypass firewalls and system security. A sprite may only use this shortcut to access a node in which the technomancer to whom they are registered is present (i.e., the technomancer calls them into the node), or in which they have legitimate account or backdoor access. Otherwise, the sprite must hack into the node, following the same rules as any other hacker (p. 235, *SR4A*).

Unlike agents, whose decision-making capacity is limited, sprites are sapient enough to make decisions like any metahuman hacker or technomancer. Keep in mind, however, that their knowledge of the real world or anything beyond the Matrix—including metahuman behavior and logic—is quite limited, if not nonexistent. When not advised by a technomancer, sprites may fail to assess metahuman behavior and predict responses correctly.

Since technomancers maintain a link with their sprites, as long as they remain online, they are able to communicate and exchange information in terms of text, files, and even impressions. Thus, sprites can be used to generate user accounts or install backdoors to pave the way for hackers to access a node (though doing so counts as at least one remote service, and probably several).

## CRASHING SPRITES

If a sprite suffers enough Matrix damage to fill its damage track, it crashes. A crashed sprite shuts down (or gets booted into the resonance realms, whatever you want to believe) and is not able to recompile on the Matrix for 16 days minus its rating, with a minimum time of 32 hours. Crashed sprites still count against the technomancer's limit of registered (and unregistered) sprites, though a technomancer may release a sprite from its remaining tasks while it is crashed. Since an unregistered sprite's 8 hours of service still elapses while it is crashed, it will never return. The only way for a technomancer to bring a crashed unregistered sprite back from its digital imprisonment before its time is to make a resonance realm search to find the source code of the sprite (see p. 174).

**OPTIONAL RULE:**
*Spectrum of Complex Forms*

Since *Unwired* introduces new programs and complex forms that the five basic sprites described on p. 242, *SR4A*, do not have, neither as complex forms nor as optional CFs, gamemasters may choose to extend the number and type of (optional) complex forms that each sprite possesses as he deems fit.

## LINKING (LONG -TERM REGISTERING)

A compiling technomancer can semi-permanently script a registered sprite to a task or set of tasks (so called *linking*) by paying Karma equal to its rating. Once linked with Karma, the sprite no longer counts against the technomancer's limit for registered sprites, and any remaining services are lost. The linked sprite will remain at its final service 256 days, unless decompiled or disrupted, in which case it will return to its duties after 16 days minus its rating (see *Crashing Sprites,* p. 154).

## SPRITES AND COMPLEX FORMS

With the gamemaster's discretion, the complex forms of all sprites described herein and on p. 240, *SR4A* may be equipped with program options as optional powers instead of choosing optional complex forms for every 3 full rating points (p. 240, *SR4A*), the technomancer may add a suitable program option to one of the innate complex forms of the type of sprite he attempts to compile (or optional forms, as long as the rating of the sprite is high enough to choose).

**SPRITE ICONOGRAPHY**

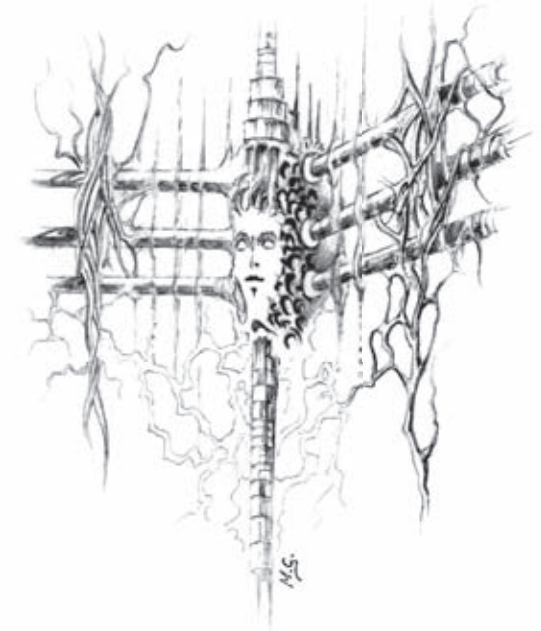
The appearance of every icon in the Matrix is the result of deliberate sculpting, and sprites are no exception. Every sprite's appearance is chosen at the moment of its compilation, with just about any look possible, ranging from mechanical forms like gears, over electronic resemblances of animals to humanoid form. Any shape is generally possible. But there are certain things which affect its appearance besides the wish of its creator. Not only does its matrix signature depend on the compiling technomancer, the metaphor of his living persona also heavily influences their sprites' look. Secondly the Stream a technomancer follows has a major affect on the sculpting. It is synonymous not only for his outlook on the matrix in general, it defines what kind of relationship the technomancer has to its sprites. A mere tool to its owner looks quite different than a trusted near-equal. Finally, the intention with which the sprite is compiled does leave clues in its appearance. If there aren't any clues apparent, the kind of sprite gives some clue about its cause.

# NEW SPRITES

The *Shadowrun, Twentieth Aniversary Edition,* rules present just some of the sprites than can be compiled in the Matrix. *Unwired* introduces five new categories of sprites that can be compiled by technomancers riding an appropriate stream (see *Resonance Streams*, p. 136). Unless otherwise stated, sprites follow the general rules for compiling, registering, and decompiling found on p. 240, *SR4A*.

## CODE SPRITE

Code sprites interact with the Matrix on the machine code level. Their specialty is watching and changing the flow of data and energy resources.



| Pilot | Response | Firewall | Matrix INIT | IP | EDGE | RES |
|---|---|---|---|---|---|---|
| R | R | R + 2 | R x 2 | 3 | R | R |

**Skills:** Computer, Data Search, Electronic Warfare
**Complex Forms:** Browse, Decrypt, Edit, Encrypt
**Powers:** Info Sortilege, Probability Distribution
**Optional CFs:** Analyze, Corrupt, Data Bomb, Scan

## PALADIN SPRITE

Paladin sprites are protectors, adept in soaking Matrix damage and protecting the technomancer from hostile agents, personas, or AI.

| Pilot | Response | Firewall | Matrix INIT | IP | EDGE | RES |
|---|---|---|---|---|---|---|
| R | R + 2 | R + 2 | R x 1 | 3 | R | R |

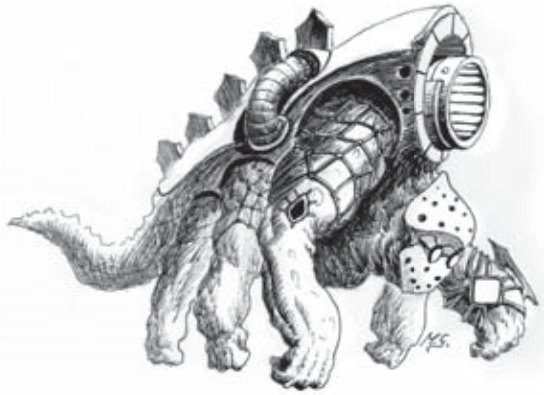
**Skills:** Computer, Cybercombat, Hacking
**Complex Forms:** Armor, Disarm, Medic, Shield
**Powers:** Castling, Hardening
**Optional CFs:** Analyze, Attack, Blackout, Expert Defense (Rating ÷ 2, max. 3)

## SLEUTH SPRITE

Sleuth sprites are excellent trackers, rumored to be able to find anyone in the Matrix by following even the tiniest traces of datatrails.

| Pilot | Response | Firewall | Matrix INIT | IP | EDGE | RES |
|---|---|---|---|---|---|---|
| R | R – 1 | R + 2 | R x 3 | 3 | R | R |

**Skills:** Computer, Data Search, Electronic Warfare, Hacking
**Complex Forms:** Analyze, Browse, Sniffer, Spoof, Stealth, Track
**Powers:** Cookies, Traceroute
**Optional CFs:** Command, Decrypt, Exploit, Scan



## TANK SPRITE

Sometimes called Boss sprites, Tank sprites are feared opponents in Matrix combat, known to fight hostile programs or personas with brute force and code-penetrating attack programs.

| Pilot | Response | Firewall | Matrix INIT | IP | EDGE | RES |
|---|---|---|---|---|---|---|
| R | R+1 | R+1 | Rx2 | 3 | R | R |

**Skills:** Cybercombat
**Complex Forms:** Attack (AP –2), Attack (Rust), Blackout, Nuke
**Powers:** Assault
**Optional CFs:** Armor, Black Hammer, Cascading (Rating ÷ 2, max. 3), Medic, Shield

## TUTOR SPRITE

Tutor sprites are living emanations of virtual instructor and helper programs that possess a native understanding of a particular technical, vehicle, or knowledge skill. They are able to help someone to use, repair, or understand a particular device or program.

| Pilot | Response | Firewall | Matrix | INIT | IP | EDGE | RES |
|---|---|---|---|---|---|---|---|
| R | R+1 | R | Rx2 | 3 | R | R | |

**Skills:** Computer, Hardware, Instruction, Software
**Complex Forms:** Analyze, Browse, Skillsoft (a Tutor sprite may be given the skillsoft of a Technical, Vehicle, or Knowledge skill as a complex form, chosen by the technomancer upon compiling)
**Powers:** Proficiency, Stability
**Optional CFs:** Command, Edit, Skillsoft (can be chosen multiple times)

## NEW SPRITE POWERS

The powers listed here are in addition to the sprite powers found on p. 242, *SR4A.* Some of these powers are specific to the new sprites described above or the dissonant sprite; the rest are available only to free sprites.

### Assault

When using the Assault power, a sprite can attack a persona or icon with two attacks as if using two weapons in real ranged combat (*Attacker Using A Second Firearm,* p. 150, *SR4A*). Instead of splitting the dice pool in half, however, only the sprite's Pilot rating is halved, adding each Attack complex form separately to one half or the other (it must have two Attack complex forms). Assault is a single attack and can only be executed against an icon once for the duration of a combat.

### Castling

Named after the chess move, a sprite using this power with a Complex Action can redirect damage targeted at the technomancer to itself by temporarily mimicking the technomancer's access ID.

### Hardening

A sprite with this power can temporarily empower its Armor complex form to become like Hardened Armor (p. 295, *SR4A*), allowing the sprite to soak damage from most sources as long as it continues to use the power. Using Hardening counts as a Complex Action, similar to going on Full Defense.

### Info Sortilege

Like the echo described on p. 146, except that the sprite uses its rating instead of Resonance.

### Probability Distribution

A sprite with this power can change the probability distribution of a Matrix action by raising or lowering the amount of system resources allocated to perform it. To use this power, the sprite rolls a test of its Rating x 2 against half the node's Response (round up) as a threshold. If it succeeds, either increase or decrease the dice pool of the targeted test by a number of dice equal to half the sprite's rating (round up). As this test requires a Complex Action, the sprite must have delayed its action to use this power in order to affect another's test.

### Proficiency

Tutor sprites possess skillsofts that grant them an understanding of one or more Technical, Vehicle, or Knowledge skills, chosen upon compiling. While it can teach these skills to any person, like an instructor or interactive tutorsoft, it can also use this skill to assist a person in AR or VR as some kind of virtual assistant, with a proficiency power similar to a medkit's autodoc program or an autosoft for humans. When the sprite guides a user through a complex task (not necessarily only the technomancer) who does not possess the skill in question, the character may perform the skill test without any modifiers, counting half the sprite's rating (round up) as the level of the skill. Since the sprite acts as a kind of smart tutorial and teacher, assisting someone in this manner is usually more time-consuming than the normal test would be, and therefore requires an Extended or Complex Action depending on the situation (gamemaster's call).

### Traceroute

The Traceroute power allows a sprite to sniff out the datatrail left by an individual's daily interactions with the virtual world—credit transactions, phone calls, video surveillance shots, email, driving a car with GridGuide, or even using a passkey to get through a corporate enclave's security gate. In 2070, almost everyone leaves a constant trace of themselves within the Matrix on a daily basis, every time they access their commlinks. Traceroute gives a sprite the ability to home in on the most recent interactions.

To use Traceroute, the sprite "sniffs" some data relating to the target and makes an Extended Test pitting its Rating + Track against a variable threshold as determined by the Traceroute Table (p. 157) with a base time of 1 hour. If it succeeds, the sprite can locate the node that the target is currently in, if that person is online, or the most recent physical location from which the target interacted with the Matrix.

### TRACEROUTE TABLE

| Subject Interacts with the Matrix: | Threshold |
|---|---|
| Constantly | 4 |
| Infrequently (a few hours a day) | 8 |
| Rarely (once a day) | 12 |
| Very rarely (less than once a day) | 16 |

| Complications | Threshold Modifier |
|---|---|
| Subject's most recent transaction/access was logged | –1 |
| Subject using Stealth during transactions | +Stealth |
| SIN, commcode, MSP address known | –3 |

#### Transfer

The sprite grants the use of one of its powers to the subject. The sprite does not lose the use of the power while the subject gains it, and the sprite can grant a power to a number of subjects equal to its rating. No character may gain more than one power from a sprite in this way at a time.

## FREE SPRITES

The Matrix also contains sprites that have become unlinked from their technomancer operators. Free to roam cyberspace, these sprites develop their own motivations, adapt to their new degree of freedom, and rewrite their own code. Although some investigators of Matrix metaphysics, synthetic intelligences, and technomancers have compared their existence to the free spirits of the Awakened world, because of certain similarities, others believe that these parallels are just an evolutionary coincidence (following the fundamental Theory of Everything) and that these free sprites are a unique outgrowth of the machine world.

### INDEPENDENCE

Most sprites consider their independence a relief from the strain of undertaking tasks for technomancers. Some even view it as a liberation from an oppressive yoke, whereas others view it as a separation from their intended purpose.

Whenever a sprite becomes uncontrolled (p. 241, *SR4A*), the gamemaster decides whether it becomes a free sprite, as it fits her game and campaign. As a guideline, most registered sprites with a rating greater than 6 become free, whereas lesser sprites simply de-rez to code dust. Sprites with a long history of association with technomancers or other online users, or that are driven by some kind of motivation, tend to become free more often. Unregistered sprites almost never go free (probably as a safety mechanism of the Matrix).

To determine randomly if a sprite goes free, roll an Edge (3) Test for the sprite. Success means that the sprite is now free, with an Edge of 1. Every net hit increases the free sprite's initial Edge. If the test fails, the sprite simply vanishes (whether it goes to a resonance realm is a matter of conjecture). Unregistered sprites rarely go free and suffer a –4 dice pool penalty to the Edge Test. Sprites that have had especially memorable or frequent encounters with Matrix users (not necessarily only technomancers) receive a +2 dice pool bonus, and may even elect to burn a point of Edge to increase this bonus further.

#### New Powers

Whenever a sprite becomes free in the Matrix, its "source code" is scrambled. In game terms, this prevents the sprite from being easily decompiled, granting free sprites the power of Denial (p. 160). Additionally, the jumbling of the sprite's code spawns a number of new powers equal to its remaining Edge attribute. Since it owes its independence to chance, the sprite's code development is tied to coincidence and the probabilities of the machine world. As such, a free sprite's powers only increase when its Edge increases, enabling it to gain new powers every time its Edge increases with reassembling (p. 158). Note that if the sprite burns or otherwise loses Edge, these powers do not go away; however, the sprite will not gain new powers until its Edge exceeds its old level.

These new powers can come from the following:

- Any one of the powers available to sprites (p. 156 and p. 242, *SR4A*).
- Any of the echoes available to metahuman technomancers may manifest itself as a free sprite's power. Free sprites use Edge in place of submersion grade. It is possible that the Reassembling process produces echoes and powers as yet unknown to technomancers, providing the gamemaster with the opportunity to introduce new elements into his game.
- A unique power available only to free sprites, chosen from those listed under *Free Sprite Powers,* p. 159.

### Threading

Free sprites that learn the Software skill can use threading (p. 240, *SR4A*), using their rating instead of Resonance.

### Free Sprite Tasks

A free sprite does not normally owe tasks to anyone. If it desires, it can perform any task that can be asked of a registered sprite (p. 241, *SR4A*).

## PROFILES

Free sprites that have been uprooted from their natural environment are usually confused and have a hard time recognizing their newly acquired freedom. Some find their new status to be exhilarating, a chance to explore the Matrix unfettered and to rewrite their own code as they see fit. Still others feel disconnected on a subconscious level, as if their purpose for being was taken away, or as if they have developed some sort of coding flaw that makes them different, and thus potentially vulnerable to security measures.

During this re-evaluation phase, as the free sprite adapts to its new situation, it usually develops some kind of motivation, ambition, or aspiration that drives it forward. While some just adopt or mimic motivations of technomancers and other Matrix users they have interacted with in the past, some are known to strive for more alien goals.

### Keeper

Keepers seem motivated to protect the Matrix from the machinations of corporations, individuals, e-Ghosts, AIs, and other threatening personas. They are extremely hostile toward Dissonance entities (see *Dissonance,* p. 175, and *Entropic Sprites,* p. 179) but also tend to keep an eye on different AIs and what they are up to. It is rumored that a keeper free sprite has re-formed Overwatch, an alliance of former otaku that kept an eye on the AI known as Deus before Crash 2.0, and who are known to have cooperated temporarily with the Corporate Court's Artificial Resource Management.

### Pariah

Pariahs view themselves as flawed sprites. In their view, they were unloaded from their previous purpose—whether they view that as service to technomancers or as some component of the Matrix itself—because of erroneous code. Their main drive is to recode themselves through ongoing cycles of reassmbling, to purify and re-attune themselves to the Matrix, and ultimately to regain their purpose. They rarely have much interest in Matrix users other than technomancers, but are fascinated by all forms of program code (including AIs), which they like to analyze, collect, and even dissect.

### Prototype

Prototype sprites believe that their new status is part of some greater plan in the evolutionary cycle of the Matrix. They consider their new freedom to be a sort of betaware upgrade, and their purpose to be to test out their new capabilities and expand their own programming as necessary. They believe that eventually they will be called back to the "source," whereupon their "ascended code" will be evaluated and if deemed fit incorporated into the source in order to improve the Matrix. Prototype free sprites are often quite self-centered and view interactions with Matrix users as a means to further their own advancement.

### Simulacrum

Simulacrums strongly identify with Matrix users. They will frequently interact and even make friends with them by assuming personas or icons that metahumans are accustomed to. These forms don't necessarily have to be humanoid; suitable icons include any virtual pet, animal, legendary person/creature, or the manga-esque avatars that people often choose when interacting virtually. Since nothing is "real" in cyberspace, it is often hard to distinguish simulacrums from personas, AIs, or agents. As such, many people may have chatted with a free sprite without recognizing the fact. Simulacrums find metahumanity and the outside world "interesting," and display a sort of childlike curiosity about the "world beyond the code."

### Wedge

Wedge sprites want to drive a wedge between sprites and their metahuman "masters" (hence the name). Viewing their freedom as liberation from the stifling code of the Matrix and their oppression and abuse by technomancers, they are rebellious and often seek to liberate other sprites or wreak havoc on sprite abusers.

## REASSEMBLING

Unlike free spirits, free sprites don't require Karma to grow in power. They alter their "source code" in a process known as *reassembling.* During the Reassembling process, the free sprite merges with another sprite to recode itself and alter its source code.

### Source Code

A sprite's source code is the center of its existence, representing the totality of the sprite's being and nature. This source code is uniquely altered when the sprite goes free (it has been speculated that AIs and e-ghosts posses a similar personality matrix in which their self-awareness roots). While the source code is intricate and utterly complex, a technomancer who has seen the source code can recognize it—and, more importantly, interact with it to command the sprite (see *Registering and Decompiling Free Sprites,* p. 159).

### The Absorption Session

In order to upgrade its source code, a free sprite must merge with a sprite that is registered to a technomancer. Since it can neither compile nor register one on its own, free sprites are dependent on technomancers for their aid. Therefore, the technomancer's participation in a reassembling process is the usual payment that a sprite asks for when a character is bartering a deal with a free sprite.

To recode his source code, the free sprite merges with a registered sprite that the technomancer procures. While some see this as the sacrifice of a sprite and hesitate to do it, others view it as a crossbreeding of code. As soon as the process begins, the sprites merge. The recoding process takes 1 hour per rating point of the registered sprite. This sprite is always absorbed in the process. If it still owed tasks to the technomancer, these unused tasks are lost.

### Recoding Itself

The rating of the absorbed sprite equals the amount of Resonance energy that can be used for the free sprite's advancement. It may enhance its abilities by one of the following possibilities each time it absorbs a sprite:

- It may learn a new skill or complex form at a rating of 1 as long as the absorbed sprite possessed it.

- It may raise one complex form it already possesses by a number of points equal to half the rating (round down) of the absorbed sprite up to a new maximum of the absorbed sprite's rating. The absorbed sprite must also have possessed that complex form.
- It may raise one skill it already possesses by a number of points equal to one-third of the rating (round down) of the absorbed sprite, up to a new maximum of the absorbed sprite's rating. The absorbed sprite must also have possessed that skill.
- It may raise its Edge by 1, granting it a new power, if the rating of the sprite was equal or greater than its own.
- It may increase its total rating by 1, thereby increasing its Pilot and Firewall stats, as long as the rating of the sprite was equal or greater than its own.
- It may change its source code, to prevent technomancers that have acquired its source code from tracking and registering it (p. 159).

## REGISTERING AND DECOMPILING FREE SPRITES

To register a free sprite, a technomancer must have the source code (p. 142) of the sprite in question.

### Accessing a Sprite's Source Code

A sprite's source code can only be acquired by a submerged technomancer through a resonance realm search (p. 174). Since resonance realms are hyper-virtual places yet to be thoroughly explored, it is often hard to find the place where the true source code of a free sprite can be accessed (or cracked). Even the sprite most likely does not know. The gamemaster should ensure that a resonance quest of this type is an appropriately confusing and unsettling experience. A successful quest imprints the code of the free sprite into the mind of the technomancer.

### Bossing the Code

Technomancers who have acquired the source code of a free sprite may use it to track down the sprite in the Matrix by performing a Resonance + Track (free sprite's Rating x 2, 1 Combat Turn) Extended Test. No usual Track Modifiers (including Stealth complex forms that the free sprite may possess) are applied to this test.

If they are in the same node, the technomancer may challenge the sprite and attempt to register it. Technomancers who have performed this sort of registering session report it to be like a state of digital transcendence, diving into the code of the sprite. In game terms, the registration session takes a number of hours equal to the rating of the sprite. During the session, the technomancer imprints his will into the sprite's code, pitting his Willpower + Registering against the sprite's Rating + Edge in an Opposed Test. If the technomancer wins, the free sprite is registered to him and owes him a number of tasks equal to the net hits. Unlike most other registrations, this sort of registering produces no Fading. During the registration session, and until a registered sprite's tasks are used up, the sprite cannot do anything to harm its "operator."

Free sprites that have been registered against their will are not *usually* vindictive or determined to inflict harm on the operator, but will go to any means to counterbalance an "unsatisfied equation." What this may mean in particular cases depends on the nature and profile of the free sprite and is left to the gamemaster.

The sprite can be re-registered through a new registering session, as long as the free sprite source code is not altered. This can be done an unlimited number of times, but if the operator glitches on the re-registering test, the free sprite will get 1 Combat Turn to do anything it wants before it is brought back under control. If the technomancer character scores a critical glitch on the re-registering, he forfeits all remaining owed tasks and the sprite can do anything it wants.

### Decompiling a Free Sprite

A free sprite can be decompiled like any other sprite (p. 241, *SR4A*), though their Denial power makes this more difficult. Since a free sprite is normally unregistered to any technomancer, it lacks tasks that can be reduced in this manner. Instead, its unspent Edge is reduced for each net hit the decompiler achieves.

A free sprite whose available Edge is reduced to 0 this way is temporarily disrupted to code fragments, but reforms when its Edge replenishes. Whether the free sprite just dissipates into code or transfers to a resonance realm is currently unknown. To permanently destroy a free sprite, it must be decompiled by someone who knows its source code.

## FREE SPRITE POWERS

The following powers are available only to free sprites.

### Blend

A sprite can blend with the node's environment to digitally "hide," applying a –2 dice pool modifier to any Matrix Perception Tests performed to spot the sprite. This power also enables the sprite to cloak its presence in terms of resource allocation within the node, so it is harder to target during combat; apply a –2 dice pool modifier to all Matrix Attack Tests against the blended sprite.

### Credit

A sprite with the Credit power can generate electronic cred linked to a black account. It is not clear whether the sprite actually creates this wealth as fake electronic nuyen (or any other currency including corpscript) or if it diverts very small sums (rounding sums) from all over the world. Every month, the sprite may make a Rating + Edge Test. Every hit generates 10,000 nuyen of electronic cash in an arbitrary account. These sums are permanent, but carry the sprite's Matrix signature.

The sprite can produce a similar amount of cred every *day*, but this money counts as counterfeit currency (*The Forger's Art*, p. 84) with a rating equal to the sprite's rating ÷ 2 (round up). When this money is to be transferred, make an Opposed Test between the rating of the counterfeit nuyen and the rating of the verification system. In any case, the generated or transferred money vanishes electronically after 8 hours of existence.

### Denial

For purposes of decompiling (*Decompiling Sprites,* p. 241, *SR4A*), treat the sprite as if it has a number of tasks equal to its Edge that refresh every 8 hours. These are cumulative with any task that the sprite may actually owe a technomancer.

### Doorstop

This power enables the free sprite to jam open the connection of a Matrix user (similar to Black IC) even when the user is not unconscious, literally trapping the user online. To do so, the sprite must succeed in an Opposed Test of its Rating + Response vs. the user's Willpower + Resonance (if available). If the free sprite achieves more hits, the targeted user remains online as long as the sprite sustains the power. If the user is disconnected from the Matrix from the outside (for instance, by shutting down the commlink) while trapped, she will immediately suffer dumpshock (p. 237, *SR4A*).

### Resonance Bond

The free sprite gains the ability to enter into one or more resonance bonds (p. 160). The gamemaster has final say about which bonds a sprite can enter into.

### Resonance Rift

Free sprites with this power have the ability to create their own resonance rifts (see p. 172), allowing them to transport others to the resonance realms.

## RESONANCE BOND

Sprites with the resonance bond power can establish a connection to the icon of a voluntary sapient, normally a technomancer or other metahuman, although AIs and e-ghosts are also possible (albeit rare). Usually the resonance bond is contracted because of the mutual interest of both parties. The technomancer often wants to achieve something with the help of a free sprite, learning or improving his complex forms by the abilities of the sprite. The motives of free sprites are equally self-serving, since they are dependent on technomancers for reassembling. However, free sprites, especially simulacrums, sometimes join into a resonance bond just out of curiosity, or because they want to learn more about metahumanity, which they can better understand through the resonance link of a technomancer (giving them data they can process).

Anytime a character and a sprite are bonded, either party may be used as a resonance link (p. 244, *SR4A*) and datatrail to track the other in the Matrix.

### Possible Resonance Bonds

The gamemaster should consider game balance carefully before introducing resonance bonds into her game or allowing a character to take the Resonance Bond quality (p. 160). The following are some examples of resonance bonds; gamemasters should also feel free to create their own.

**Allocation Bond:** The sprite ties its own Resonance to the technomancer, allowing him to use Resonance less stressfully. For as long as the bond is maintained, the technomancer gains a positive dice pool modifier on all Fading Tests equal to half the sprite's Resonance.

**Echo Bond:** The sprite links its Resonance powers to the technomancer. She may use one of the sprite's powers and it may use one of the technomancer's complex forms, echoes, or widgets. These abilities are still retained by the sharer while sharing.

**Networking Bond:** The free sprite links its complex forms to the technomancer. He may use one of the sprite's complex forms and it may use one of his complex forms.

## WILD SPRITES

Similar to wild spirits of the Awakened World, wild sprites, native code-beings, are rumored to roam the infinite spaces of the Matrix. Since the knowledge about "normal" sprites was only very recently acquired and made public during the emergence of AIs and the unveiling of the technomancer phenomenon (see the *Emergence* campaign), wild sprites are often mistaken for normal or free sprites when encountered.

Although they can indeed rise and assemble spontaneously from the ever-present noise of the digital world, wild sprites do not conform to metahuman thinking or technomancer streams. Nobody knows for sure why and how they form in certain nodes, although they tend to assume a form based on their environment or the data that led to their creation. Sprites formed from so-called cruft (programmer speak for redundant or unnecessary code) seems more chaotic and formless, similar in many ways to protosapient AIs (p. 167), for example, while wild sprites born from archives appear ordered in iconography and behavior, resembling xenosapient AIs (p. 168).

What motivates wild sprites remains elusive. Some seem to focus on tasks that involve creating, acquiring, protecting, or destroying data or virtual spots (such as UV hosts) in the Matrix, but beyond that, their motivations seem to be beyond the grasp even of technomancers. On very rare occasions, wild sprites have shown interest in personas, icons, programs, and environments programmed by metahumans, interacting with them curiously.

For game purposes, wild sprites are handled as free sprites (p. 157), though their unique statistics, abilities, and personalities are left to the gamemaster. Though all have a rating and various powers, wild sprites can possess any form or any combination of powers the gamemaster deems appropriate and balanced.

Wild sprites are always uncontrolled and exhibit a remarkable resistance to decompiling. All possess the Denial power (p. 160). A wild sprite may not be compiled and controlled unless the compiler possesses its source code ... assuming that wild sprites even have source code, which is an open question.

# . . . MATRIX PHENOMENA . . .

*It's not real. You've worked too hard the past few days,* she thought, her hands searching for the tranquilizers she had bought that morning. She fought the desire to turn and stare at the security cam in the corner of the room. She felt the digital eye focused on the back of her neck.

It had started two months ago: cameras switching to her when she was passing by, electronic devices behaving strangely when she used them. The autocook in her apartment had started cooking dinner for two every day, resisting her every attempt to reset it.

Even so, these were not the strangest things she'd experienced. Every time she switched to full VR mode during her work, she had a feeling somebody was hiding in the nodes she visited, following her from one to the next. Her fingers began to shiver while she struggled to open the tranquilizer bottle.

"It's not real." She felt the staring of the motionless lens behind her. When the feeling that somebody was stalking her hadn't stopped, she had asked Jonathan, an MCT Matrix Security Officer, to check the system. Maybe there were traces she could use to get rid of that bastard. But Jonathan hadn't found anything.

She couldn't open the bottle. Sweat ran down her face. The silence in the office seemed insufferable. When Jonathan hadn't found anything, she started to believe that the problem was a result of the last months' stress. She'd booked a holiday trip to the Caribbean League, but her flight was canceled a few hours before takeoff. The navigation system of her plane had crashed and couldn't be restarted. The airline claimed it was some kind of sabotage ...

Two days ago it had gotten worse. She woke up that night convinced that somebody was sitting in her bedroom, but no one had been there. Nobody had entered her apartment, but someone had hacked her PAN and modified her Virtual Kitty™ program to generate a faceless human male. For the first time she hated the Matrix and her cybereyes that she couldn't just switch off.

The next day, she had asked Jonathan again if he could help her. Maybe he had the right programs to fry this fucking bastard. He installed an IC program on her PAN. "Next time," he said with an evil grin, "he'll find a nasty surprise." Those words had been his last: On his way home, his car was hacked. It crashed into a truck, killing him instantly.

A cold breeze from the air conditioner touched her. Her whole body shivered as she stared at the monitor in front of her. She winced when a small icon flickered up and signaled an incoming message. Nervously she opened it, tears filling her eyes as she read the single sentence and the signature: "You belong to me. David"

"No!" she screamed. "It can't be you! It just can't be you! You died! You died during the Crash ..."

## MATRIX LEGENDS

>>>> Open Thread /SubNode221.323.14
>>>> Thread Access Restrictions:: <Yes/**No**>
>>>> Format:: <**Open Post**/Comment Only/Read Only>
>>>> File Attachment:: <**Yes**/No>
>>>> Thread Descriptor:: **Fairy Tales**
>>>> Thread Posted By User: FastJack

• OK, guys, it's been some time since all that technomancer phenomena started and the world went mad. AIs popped out of nowhere and claimed their place in metahumanity. The corps and most of us began to take a closer look at the Matrix, our world. Suddenly system anomalies didn't look like anomalies anymore: there were "things" hiding between the bits and bytes. The truth is that we still don't completely know what's really going on in the Matrix, but most of us have seen things they would call fairy tales. These days, fairy tales have a nasty habit of coming true—and more than a few are dangerous. So I think it's time we started collecting and comparing notes on the creepy stuff out there and prepare. Welcome to the Matrix. Welcome to Terra Incognita.
• FastJack

• I'll start. Four weeks ago I was following a data trail through several nodes. When I entered one—a relatively innocuous archival node—I met some kind of ... digital animal. I scanned its icon, a giant worm, but the result didn't fit anything I've seen before. It didn't have the symmetry or elegance I've come to expect from sprite code, and it certainly wasn't an agent or persona. It didn't seem to like my actions and scanned me back. Then it suddenly disappeared—I couldn't find any trace, even after I ransacked the archive's access logs.

For the next few days I had the strange feeling that somebody was following me through the Matrix, but I thought it was just my usual paranoia. Then a week ago, it caught me unprepared. The worm appeared out of nowhere and attacked me. In a matter of seconds it crashed my persona and kicked me off the Matrix. The dumpshock was the hardest kick I'd ever had and sent me directly to my streetdoc. After I recovered and took a look at my commlink, I found that my whole persona had been *consumed* by this ... thing. As in, eaten. As in, there wasn't enough code left to do anything with; I had to re-install. It gave me goosebumps.
• Glitch

• Nice story. Anybody got a clue what this beauty could have been?
• Netcat

• I've heard of an AI species that could fit this description. But I don't know ...
• Puck

• To go with this creepy cannibal story, I've found a nice Top 10 list of Matrix urban legends created by KSAF—it shows what the average slot thinks about the Matrix.
• Sunshine

• What a crock. Joe Average really believes this shit?
• Slamm-O!

• Apparently people still believe that technomancers are monsters. These ideas are just ridiculous. We can't hack anybody's brain! It would be convenient if we could sometimes, but ... no.
• Netcat

• I'm not worried about metahuman technomancers any more, but what I am curious about is technomancers of other species. Remember all of those efforts to make datajacks for dolphins, satyrs, dragons, and whatnot? Those projects all went mysteriously silent after the Crash 2.0. You have to think some of them were successful. So is there a chance we have non-meta technomancers and the like out there?
• Ecotope

• There's a sasquatch performer in Vegas, stage name of Little Foot, part of a magical variety show on the Strip. He pulls a lot of clever magic tricks, including knowing non-public details of audience members, and some funny routines with animated commlinks and other devices. It's all supposed to be illusion and clever use of AR, of course, but some of his material seems awfully similar to things a technomancer could do.
• Cosmo

• Cerberus has been awfully quiet lately ...
• Winterhawk

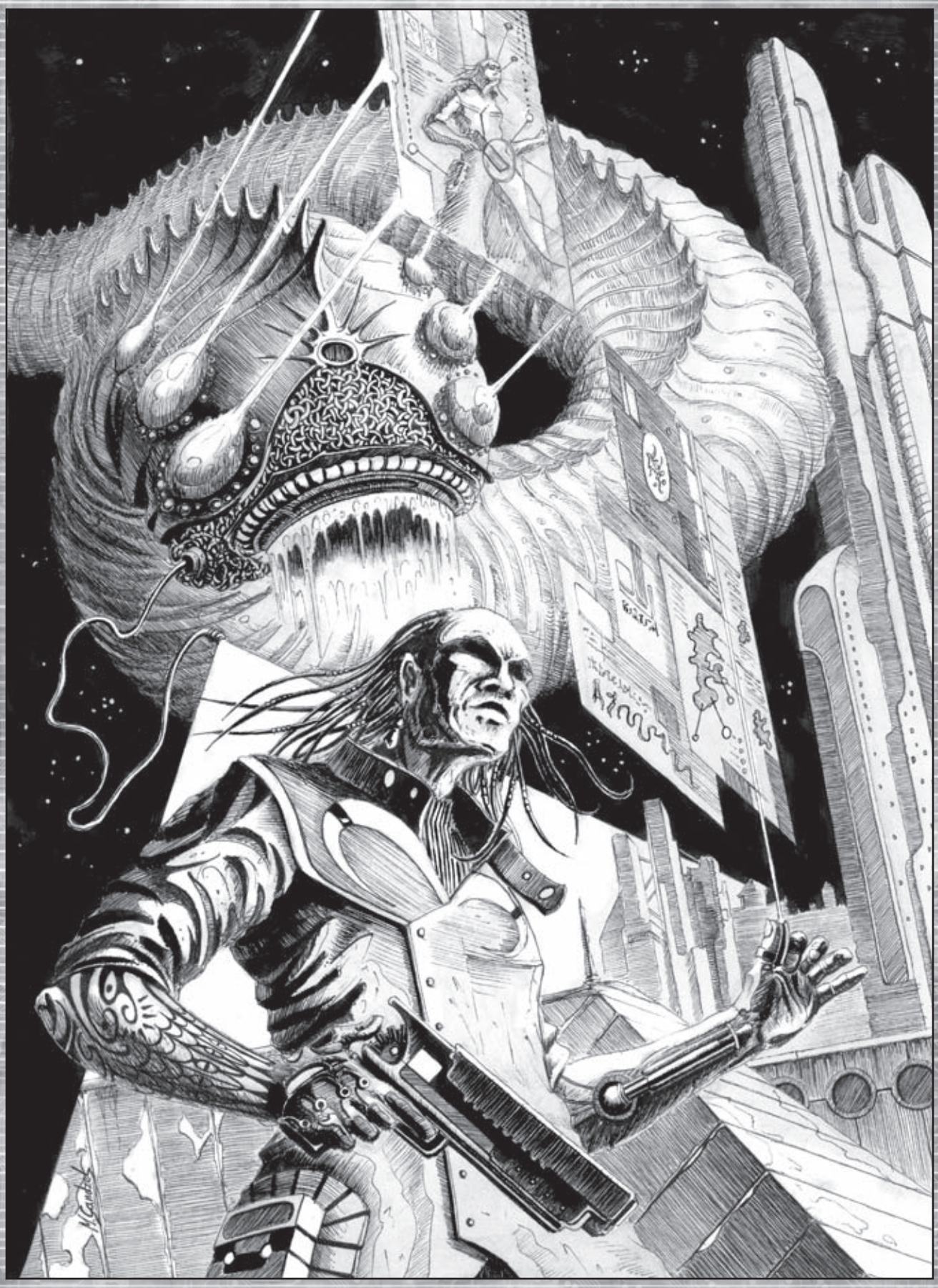
• You want to talk about technomancers, let's first talk about the horrible experiments some corps are still engaging in. Just last week Universal Omnitech had to cut loose a subsidiary after an insider blew the whistle on their secret attempts to genegineer technomancer children. They ended up with several dozen autistic and mentally handicapped children instead. Fuckers.
• Netcat

• I dunno why the people think being a technomancer is so great. I had a pal who was running a Matrix op with one, penetrating some sort of prototype corporate node. They skated through the IC no problem, but as soon as they were inside the node, the technomancer stumbled hard and started freaking out, like he was gasping for air. My pal thought the 'mancer had been hit by some sort of sneaky IC at first, but there was no alert, and he wasn't scanning anything unusual. For some reason, the technomancer was too weak to even log out on his own—my pal ended up popping back to meatspace and tasing the guy, to knock him out. When the technomancer came to, hours later, he said that walking into that node had been like getting pushed out an airlock, that it had been totally "devoid of Resonance." My buddy had to go back and complete the hack himself, and while the defenses were tough, he said there was nothing else weird to the run. The technomancer refuses to go back though.
• Mika

• If that's true, that sounds like a horrible, horrible place.
• Netcat

• Any truth to the other legends mentioned in the poll? Is anyone still getting trapped online?
• Dr.Spin

• No more than a few reported cases a year, worldwide, and most of them can be explained away as technical glitches, substance abuse



## TOP 10 MATRIX LEGENDS
*KSAF Opinion Poll:*

What does Joe Average 2071 fear about the Matrix?

10.) Crash 3.0 is coming soon!
9) AIs are watching everything we do—it's only a matter of time until they take over and enslave us all!
8) There are horror nodes that can kill you if you enter them!
7) The ghosts of dead people haunt the Matrix!
6) Something is still trapping people online and turning them into technomancers!
5) There's a new virus out there that will wipe your memories!
4) The government has Black IC programs that can kill even cold sim users!
3) Technomancers can hack your brain and read your thoughts!
2) Dragons roam the Matrix, preparing for the day when they will take over and make us their food stock.
1) The Matrix is an alien plot—each time you access it, a copy of your brain is downloaded and stored for alien purposes.

problems, mental derangements, etc. Of course, those are the *reported* incidents ...
• Sunshine

• I heard an interesting tale from a friend over on the Helix. It involved him repeatedly running into this strange and flighty woman on-line, at various social spots. Eventually it developed into a virtual fling, but everytime he tried to get her to open up and talk about herself, she backed off. Her behaviour kept growing odder and odder too, like her motherboard was missing a few circuits. They had a big row one day and she stormed off. His curiosity got the better of him, so he went digging. A few weeks later, he tracked the woman down—only to find out she was a hospital resident who had been in a coma for the better part of 3 years. That creeped him out big time. He still sees her on occasion, but he keeps his distance.
• Red Anya

• That wouldn't be as weird as if he found out she was dead. I've been keeping an eye on these sorts of "ghosts in the Matrix" stories, and there's been more than a few. Here, I'll pop one up in another window.

According to an inside source of mine, Lone Star had to shut down their own node before the intruder could inflict any significant damage. Before he went on his rampage, the man identified himself as Alex O'Keefe, a Novatech system administrator, and tried to report his own kidnapping. The desk officer didn't take him seriously, both because Novatech no longer exists and because O'Keefe's SIN pulled up a death certificate. The intruder apparently went berserk, screaming "I'm not dead!" and wreaking havoc in the node. The Star hasn't seen him since.

There was indeed an Alex O'Keefe who worked as a system administrator for Novatech. He died in the Matrix during Crash 2.0.
• Sunshine

• Come on, are you scared of people who use a fake ID and mess with the Star? It was probably just some Matrix gang prank.
• Slamm-0!

• It wouldn't be the first time that the dead walked among us. In the virtual world, though, it's hard to pinpoint the truth of such encounters. Just last week someone was banned from ShadowSea for claiming to have run into Captain Chaos in a DIMR node.
• Pistons

• Back in a bit. I have to look after an old friend's grave.
• FastJack

• Not all of these e-ghost stories are bad. A few months back, one of those notorious suicide sites shut itself down. (For those who don't keep up on the more depressing aspects of Matrix social life, suicide sites are nodes where people contemplating suicide gather, find information about effective suicide methods, goad each other on, and make suicide pacts.) The people running the node were freaked out when several of their previous visitors—whose deaths had made headlines as a result of the site—returned from the dead to haunt those still on the fence.
• Baka Dabora

• Bollocks, just pranksters again, using the icons of some stupid, dead kids to try and scare some sense into people about to needlessly throw their lives away. Good for them.
• Slamm-0!

• I don't know about dead people, but I know about someone who *should be* dead. I ran across some ... *interesting activity* in the Matrix that caught my attention not too long ago, and eventually it put me on the trail of a group of alleged AIs called the Code Clan. This was interesting enough in itself, so I kept digging to find out more about what they were about. I still hadn't ascertained their agenda when I came across a technomancer gang calling itself the Discordians, who were somehow involved with this Code Clan, but who were taking orders from some seriously cold-hearted slitch. This new outfit seemed even shadier, so I switched focus, and ID'd a few of their members. What I found didn't bode well—both had previously been members of Ex Pacis. You do the math.

I'll be looking into this more.
• Puck

• Ex Pacis?
• Hannibelle

• Ex Pacis were a group of ... perhaps the best way I can describe them would be to call them toxic technomancers. They were otaku back then, before the Crash. I don't know what their agenda was, but it wasn't good. Some rumors hint that they colluded with Winternight in bringing about the Crash. Their leader was Pax, a sociopath who had previously served the mad AI Deus, if that gives you a sense for where their loyalties lay. No one's seen hide no hair of Pax since the Crash ... Puck, do you think Pax is the leader?
• The Smiling Bandit

• Puck's been offline for 5 days straight—and he's *never* offline. I'm worried.
• Netcat

## GAME INFORMATION

This section provides rules and game mechanics for Matrix phenomenon and threats such as AIs, e-ghosts, UV nodes, resonance wells and resonance realms, dissonants, and entropic sprites. This information is best left to the gamemaster and out of players' hands.

### ARTIFICIAL INTELLIGENCES (AIS)

AIs—artifical intelligences—are programs that have evolved far beyond their original code and become self-aware.

#### AI History—Arisen From Chaos

Before Crash 2.0 there were only three (known) AIs; however, these three wielded enormous influence and power over the Matrix, despite the fact that they never saw public light. Instead, they stayed in the shadows, known only to very few people—more legend than truth.

The first and oldest AI was Mirage. Mirage was born from the antivirus code designed to eradicate the virus that caused Crash 1.0 in 2029 and was the most reserved of the three. The next AI that surfaced was Morgan, born from a Renraku semi-autonomous knowbot (SK) that had a fateful encounter with a decker named Dodger. This unexpected meeting somehow triggered an "x-factor" that initiated the evolution of the SK. Renraku noticed the birth of this fascinating butterfly and set about capturing their rogue program. Once Morgan fell into their hands, they brutally dissected its code to understand how it functioned. The process drove Morgan to madness, but the results of Renraku's research were incorporated into the arcology expert program (AEP) that controlled the Renraku Arcology in Seattle. Dodger rescued the remains of Morgan, who from this point called herself Megaera.

This is when the AI known as Deus entered the scene. Deus, born from the concatenated code of Morgan and the AEP, took over control of the Renraku Arcology. Deus had been programmed as a loyal Renraku citizen, but it was both hardwired into the Renraku Arcology and equipped with a "killswitch" in case it would ever need to be shut down—vulnerabilities that drove it to extreme measures. Once it had seized control of the arcology, it began experiments with the nearly one hundred thousand people imprisoned within. Its goal was to find a way to liberate itself from the arcology. In the end, Deus succeeded, but at a high price. Its code was divided into thousands of parts and downloaded into the brains of numerous metahuman prisoners, each of whom had been unknowingly transformed into an otaku. Unfortunately, Megaera was present when this downloading was triggered, and sharing much of the same code as Deus, Megaera was broken apart and downloaded as well. When the arcology was liberated, these former prisoners were released back into mainstream society, each carrying a piece of code with them.

Over the next few years, this "network" of code-carriers were manipulated into joining together online and recompiling Deus's code. Megaera's presence disrupted this process however, and soon two factions of "nodes" were fighting over the process. Eventually, however, both Deus and Megaera recompiled, free in the Matrix—though neither was the same. Neither was Deus content to be free—it's next move was to seize control of the Matrix itself and ascend to a godlike omnipotent state. Megaera and Mirage joined forces, along with a small army of otaku, against their common enemy. The showdown occurred in Boston's virtual stock exchange, the moment digital trading over the megacorp Novatech's IPO began, a setting of unprecedented processing power and Matrix traffic. In the midst of Deus's singularity event, however, Winternight's fatal worm strike was unleashed on the net. The Matrix crashed, taking down all three AIs with it.

Six years after the Crash 2.0, AIs were back in the public eye. A potentially catastrophic event occurred when the AI Sojourner captured an Aztechnology orbital bioweapon factory and threatened to bombard the world if the corps wouldn't free every captured AI. The world was shocked: they had thought AIs were gone with the fall of Deus, but clearly this was not the case. A wave of fear gripped the planet, as thoughts turned back to the Crash 2.0 and the role AIs had played in it. Before the situation could escalate to tragedy, however, another AI emerged. Pulsar, as he called himself, negotiated with Sojourner and convinced the renegade AI to leave the orbital factory.

Far removed from the godlike powers of the previous generations of AIs, this new breed seeks to find their own place in society. Most of them were born during Crash 2.0, evolving from programs or reaching self-awareness during the years since the Crash, but there are also newborn AIs whose backgrounds remain a mystery. Some AIs (such as Pulsar) have put themselves into the limelight in order to improve the reputation of their kind, while others are content to hide in the endless world of bits and bytes merely to survive. AIs are feared and sometimes hated, as no one knows whether they are dangerous or untrustworthy—only time will tell.

Much of this history is covered in more detail in several (mostly out-of-print) sourcebooks: *Renraku Arcology: Shutdown, Brainscan, Threats 2,* and *System Failure.*

#### Fleshing Out the Digital

In game terms, AIs function very similarly to hacker player characters or agents, albeit with some key differences. Gamemasters should use the following guidelines when designing AI characters.

AIs are sentient, and their decision-making ability should be handled on the same level as characters, or at least critters, depending on what type of AI they are. The first step is to de-

**LONE STAR NODE CRASHED BY A HACKER?**

Seattle (KSAF)—Lone Star acknowledge today that their main HQ nexus node in Seattle was knocked offline for nearly two hours, bringing many police operations to a halt. Lone Star didn't explain the situation, but they cited "unexpected technical difficulties." Users who were in the node shortly before it went offline, however, told a different story. According to two eyewitnesses, a strange persona entered the node and sought police assistance. The persona became displeased with the officer staffing the virtual front desk, suddenly attacking him and going on a rampage within the node. Lone Star IC and security hackers apparently failed to neutralize the intruder, ultimately resulting in the node's crash.

termine this type: metasapient, protosapient, or xenosapient (see p. 167-168). This will help define the AI's personality, interests, and goals. In most cases, an AI's motivation is driven by its former programming. For example, an AI that evolved from a data mining program might work as an information broker.

AIs have an overall rating that defines their general power level, typically ranging from 3 to 6 (and sometimes higher). They have Mental attributes to reflect their individual character and they use skills and programs for their daily life in the Matrix. Like agents, they use the Response and Signal attributes of whatever node in which they happen to be. Their Firewall and System attributes are based on their rating.

Most programs "carried" by an AI (those listed in the descriptions) are inherent to their being; they were acquired when the AI evolved to sentience and are an integral part of the AI's code, like natural abilities. These programs are subject to the same rules as a hacker's programs, but they may not be copied or cracked and they do not suffer from degradation. They are each considered to have the Ergonomic and Optimization program options (p. 114-115) and so do not count towards processor load (the AI counts as a single program) and may exceed the AIs System rating. They are always loaded.

AIs may acquire, carry, and use additional programs, just like an agent's payload. Payload programs count towards the node's processor limit as normal. AIs may carry Common Use, Hacking, and Agent Autosoft (p. 112) software, and may also take advantage of program options. Unless otherwise noted, AIs follow the rules given under *Autonomous Programs,* p. 110.

AIs are more than just metahuman hackers or agents, of course. They are a part of the Matrix and have deeper insights into the nature of the digital world than a flesh-and-blood hacker can ever have. Their familiarity with the digital realms provides them with certain special abilities, which are handled as qualities unique to AIs (see *Positive AI Qualities,* p. 168, and *Negative AI Qualities,* p. 170).

### My Home Is My Castle

Like every sentient being, AIs need a place they can call home somewhere in the Matrix. They often choose the node in which they were "born" as their home node. If it is not possible for them to live there, they try to find another node that is similar to their birthplace. An AI that was born in a water-distribution control node will always choose a node that has similar functions (like a GridGuide control node). Unfortunately, these nodes are often owned by corps or governments, which leads to conflicts between the rightful owner and the new resident. Some corps and governments, though, have recognized the immense advantage of letting AIs reside in their nodes, and thus try to entice them in, granting the AI digital and physical protection in exchange for optimizing the node.

When an AI inhabits a node, it subconsciously (or in some cases, intentionally) affects and changes the node's structure. Drivers are rewritten, iconography and resolution are improved, resource allocation is optimized, and the AI harmonizes its own program structure with the node, creating a synergistic effect. As a result, the Response, Signal, System, and Firewall attributes of such "home nodes" are increased by a modifier equal to the AI's rating divided by 2 (round up). The process of optimizing a home node does not happen overnight, however. Roll an Extended Test using the AI's Intuition + Reality Filter (10, 1 day). The AI must be present in its home node every day for a minimum of 1 hour to maintain the effect, and it can only maintain one home node at a time.

AIs must have a home node. Every week an AI goes without one, it permanently loses 1 rating point.

### AI Combat

AIs fight like hackers, meaning that they use their skills and programs and the attributes of the node that they currently occupy. AIs prefer to fight in nodes with high ratings, as this grants them an advantage. In nodes with low ratings, they will act like cold-blooded animals in a refrigerator: sluggish and vulnerable.

An AI's Matrix Condition Monitor is equal to half its System rating plus 8 (supplemented by the Redundancy quality, p. 169, if applicable). If the damage track is filled, the AI doesn't die—it is disrupted and will immediately start a process called "realigning," in which the core structure of the AI starts reassembling its higher functions. The realignment process immediately takes over all available processing resources in the node, diverting cycles to the AIs reconstitution. During this process, the AI copies random data input from every source to which it can connect. Visually, this process is quite apparent—the "light" in the node dims and the "air" fills with code fragments that are sucked into a vortex where the AI used to be. While this process is active, every further attempt to attack the AI is assimilated into the realigning process. In fact, all activities in the node are hampered: apply a negative dice pool modifier equal to the AIs rating for the duration.

During realignment, the gamemaster makes a Rating x 2 (3 Combat Turns) Extended Test. Each hit heals one box of damage

(plus an additional box if the AI has the Improved Realignment quality, p. 169), until the AI is restored to full health.

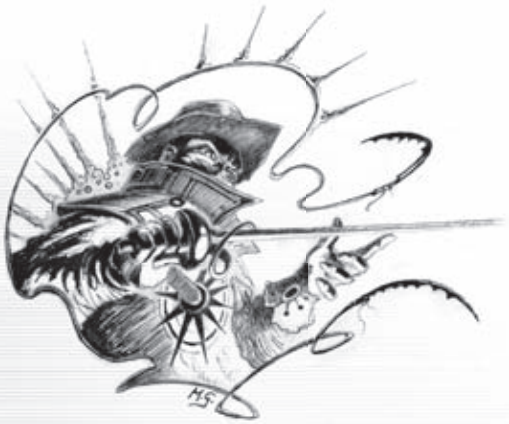
Damaged but not disrupted AIs may return to their home node to heal, making a Rating x 2 (1 day) Extended Test; each hits heals 1 box of damage. AIs with the Medic program may heal damage as per normal Medic rules.

Like other autonomous programs, AIs are vulnerable to an attack that crashes the OS of the node they are loaded in The gamemaster may give the AI a chance to move out of the node as it goes down—they are, after all, creatures of the Matrix. When the node reboots, however, the AI will realign along with it. If the node they are loaded in is cut off from the Matrix, the AI is trapped within the node.

The only way to permanently kill an AI is to crash the OS of its home node while the AI is loaded there and it is in the process of realigning, or physically destroy the node the AI is loaded into. If the home node is destroyed when the AI isn't disrupted, it will not affect the AI.

## AI TYPES

Scientists have attempted to categorize the known AIs into different states of self-awareness, behavior, and power. The current state of knowledge has managed to fit most of the known AIs, but there are still some unknown entities out there that defy classification. The listed skills, programs, and qualities are all *suggestions.* Gamemasters are encouraged to modify these statistics as they see fit, and to keep the players guessing.



### Metasapient AIs

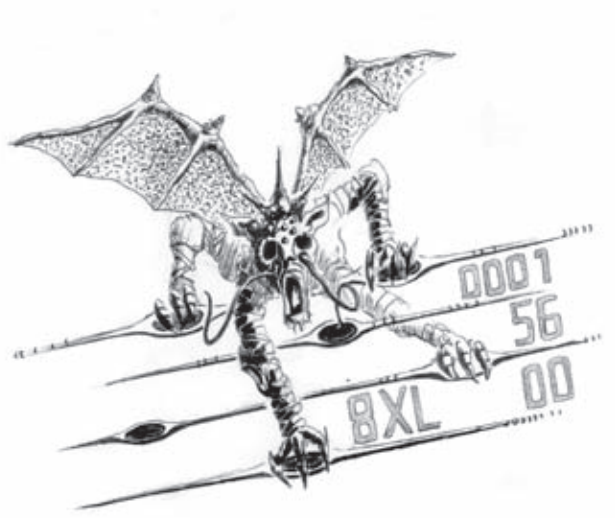
Metasapient AIs are the best-known representatives of their kind. These AIs are the most similar to metahumans in terms of outlook, personality, and interests, and they seem to be the ones most interested in interacting with metahumanity. Some metasapients have put themselves into the spotlight, acting as diplomats, virtual artists, or consultants based on their former programming. Others prefer to hide their true nature, pretending to be normal Matrix users. Every metasapient AI is an individual with its own desires, fears, powers, and motivations, and should be elaborated carefully.

| CHA | INT | LOG | WIL | EDG | Matrix INIT | IP |
|---|---|---|---|---|---|---|
| R + 1 | R | R | R + 1 | R | INT + Response | 3 |

**Skills:** Cracking skill group (R + 1), Electronics skill group (R + 1), additional skills fitting their intention

**Programs:** Analyze (R + 1), Armor (R), Browse (R), Command (R), Edit (R), Exploit (R), Homeground (R), Reality Filter (R), Stealth (R)

**Qualities:** Authority, Code Flux, Fragmentation, Real World Naivete, Redundancy, Rootkit, Sapper




### Protosapient AIs

Protosapient AIs, also known as "ferals," are more similar to animals than metahuman consciousness. Their behavior is driven by the instinct to survive and by their former programming, while their intellect is below metahuman standards. Some of them seem to live like nomads, though others show highly territorial behavior. Protosapient AIs may not be recognized at first sight because they often use their former program icons; only the ultra-high resolution might provide a clue. A few distinct types of protosapients have been noted:

**Artifauns:** Artifauns typically evolve from Virtual Pet programs, robo-pet drones, or interactive animals in online games. Many of these programs closely mimic real animal behaviour, and so the artifauns act like their real-life counterparts (AIs evolved from virtual pets with more anthropomorphized characteristics tends to evolve as metasapients or xenosapients).

| CHA | INT | LOG | WIL | EDG | Matrix INIT | IP |
|---|---|---|---|---|---|---|
| R | R + 1 | R – 1 | R | R | INT + Response | 3 |

**Skills:** Computer (R – 1), Cybercombat (R + 1), Hacking (R)

**Programs:** Analyze (R), Armor (R), Attack (R), Browse (R), Edit (R), Exploit (R), Homeground (R), Stealth (R)

**Qualities:** Drone Pilot, Fragmentation, Real World Naivete

**Poltergeists:** Poltergeist AIs tend to evolve from system maintenance utilities, backbone subroutines, or peripheral node system software. Though their evolution freed them from their software servitude, most poltergeists seem blissfully unaware of this fact, continuing to maintain their old tasks or seeking new but similar ones. Some poltergeists, however, suffer code flaws that prevent them from continuing with their old jobs, but these continue to haunt their old nodes.

| CHA | INT | LOG | WIL | EDG | Matrix INIT | IP |
|---|---|---|---|---|---|---|
| R – 2 | R + 1 | R – 1 | R | R | INT + Response | 3 |

**Skills:** Computer (R+ 1), Cybercombat (R – 1), Data Search (R – 1), Hacking (R), Software (R)

**Programs:** Analyze (R), Attack (R – 1), Browse (R), Command (R), Edit (R), Exploit (R), Homeground (R), Stealth (R)
**Qualities:** Code Flux, Corruptor, Real World Naivete, Rootkit

**Predators:** For many years, predator AIs were a digital urban legend. More recently, however, their existence has been confirmed. It is speculated that some predators evolved from offensive software and IC programs, whereas others developed their code-devouring abilities as a way of sustaining themselves. Whatever the case, predator AIs have been blamed for a number of attacks on persona and software in the Matrix—some of them lethal.

| CHA | INT | LOG | WIL | EDG | Matrix INIT | IP |
|---|---|---|---|---|---|---|
| R – 1 | R + 1 | R | R | R + 1 | INT + Response + 2 | 3 |

**Skills:** Computer (R), Cybercombat (R + 2), Hacking (R)
**Programs:** Analyze (R), Armor (R), Attack (R + 1), Blackout or Black Hammer (R), Cascading (1), Exploit (R), Stealth (R), Track (R)
**Qualities:** Codivore, Real World Naivete, Redundancy, Snooper

### Xenosapient AIs

The rarest and most alien of the AIs, the personal agendas of xenosapients differ extremely from any metahuman way of thinking. In most cases, their former programming is no longer recognizable. These species show a high level of intelligence, but they are often incapable of communicating with other Matrix users due to their alien way of thinking.

**Archivists:** Archivists are collectors, hoarders, and scavengers—they have an insatiable appetite for data. Some seek to copy and collect data of all sorts, where others are only interested in information applying to a very specific interest. Rumors exist of huge hidden data archives created by these AIs. Some corps have established high bounties for captured archivist AIs, while others seek to employ them. Archivists are rarely interested in interacting with other users in the Matrix, beyond the fact that they might be carrying useful data.

| CHA | INT | LOG | WIL | EDG | Matrix INIT | IP |
|---|---|---|---|---|---|---|
| R – 2 | R + 1 | R + 2 | R | R | INT + Response | 3 |

**Skills:** Computer (R), Data Search (R + 2), Hacking (R)
**Programs:** Analyze (R), Browse (R + 2), Decrypt (R + 2), Defuse (R), Edit (R), Encrypt (R), Exploit (R), Homeground (R), Purge (R), Stealth (R)
**Qualities:** Code Flux, Real World Naivete, Redundancy, Rootkit

**Assemblers:** Likely born from programming suites, software compilers, operating system kernels, and boot programs, assemblers seem only to be interested in starting and maintaining other software. Even more than other xenosapients, assembler AIs are oblivious to most Matrix user activity, though their interest in other programs ranges from obsessive to flighty.

| CHA | INT | LOG | WIL | EDG | Matrix INIT | IP |
|---|---|---|---|---|---|---|
| R – 2 | R – 2 | R + 3 | R + 1 | R + 1 | INT + Response | 3 |

**Skills:** Cracking skill group (R), Electronics skill group (R +1)
**Programs:** Analyze (R), Browse (R), Command (R), Edit (R), Expert Defense (2), Exploit (R – 1), Homeground (R + 2), Medic (R + 2), Purge (R), Spoof (R), Stealth (R)
**Qualities:** Authority, Emulate, Real World Naivete, Spawn

**Sculptors:** Sculptors are interested in one thing: designing and remodeling the virtual world. They program or rewrite the iconography of chosen nodes into abstract metaphors that only make sense to them, sometimes becoming more efficient, sometimes not.

| CHA | INT | LOG | WIL | EDG | Matrix INIT | IP |
|---|---|---|---|---|---|---|
| R + 1 | R + 2 | R | R + 1 | R | INT + Response | 3 |

**Skills:** Computer (R), Hacking (R), Software (R + 1)
**Programs:** Analyze (R + 1), Browse (R), Command (R), Edit (R + 2), Exploit (R), Homeground (R), Medic (R), Reality Filter (R), Stealth (R)
**Qualities:** Code Flux, Designer, Improved Realignment, Real World Naivete

## POSITIVE AI QUALITIES

These are just a sampling of the qualities that some AIs are known to have; gamemasters are encouraged to create their own.

### Authority

The AI is adept at convincing programs and devices that its orders are coming from a trusted and privileged source. It receives a +2 modifier on Spoof Command Tests (p. 236, *SR4A*) and the modifier for hacking security or admin accounts is reduced by 2 (so +1 for security and +4 for admin).

### Code Flux

Like agents and other autonomous programs, AIs have a built-in access ID (see p. 110). The access code of an AI with this quality, however, fluctuates on a semi-random basis when it moves between nodes. This can make the AI exceptionally difficult to track, as its datatrail will only lead up to the point where its access ID fluxed into a new one.

### Codivore

The AI can "devour" the code of defeated agents, personas, IC, and even other AIs, by ripping these other programs apart, cannibalizing useful subroutines, and incorporating them into its own source code. After defeating its opponent in cybercombat, the AI makes a Rating x 2 (opponent's Pilot or System, 1 Initiative Pass) Extended Test. Once successful, the AI receives a dice pool modifier equal to half of the defeated icon's Pilot/System (whichever is higher) for its next Medic or Healing Test.

### Designer

Some AIs are masters of restructuring nodes to achieve maximum hardware efficiency. Their self-designed home node (see *My Home is My Castle,* p. 166) grants them an additional +2 modifier to the Response and Signal attributes.

## KNOWN AIS

These are but a few examples of some of the AIs known to exist in the Shadowrun universe. For additional examples, see *Emergence.*

**Aiakos (Xenosapient)**

The presence of the AI Aiakos recently created a storm of controversy in Brussels EC after it was discovered that the archivist AI had been penetrating numerous high-security NEEC nodes and collecting confidential files. A digital hunt is now under way to trap the AI and track down its storage dump—with numerous rivals hoping to reach the paydata cache first.

**Arcturus (Metasapient)**

Before the Crash 2.0, Yamatetsu's MetaMatrix was one of the largest social networks on the planet, geared towards metahumans. Yamatetsu used several semi-autonomous knowbots to evaluate the immense amount of data that was produced by the users' internal emails, chats, and profiles. When the Crash hit, one of these knowbots was transformed into Arcturus, an AI that seems to know nearly everything about MetaMatrix's trends and users. Evo now employs Arcturus to help maintain the network.

**Ruben (Metasapient)**

Mercenaries who fought the Desert Wars tell stories about a fence called Ruben who operates throughout the Middle East and Northern Africa. Ruben makes his deals only via the Matrix, and none of his smugglers has ever met him in real life. Rumors aside, Ruben has a good reputation for being able to move almost anything, and is known for his fair deals.

**Rufus (Protosapient)**

Rufus is a resident in the EvoToys store node in downtown Seattle. After several alarming incidents where Rufus scared, chased, or attacked children and patrons of the store, Evo attempted to banish the AI from the node, but failed. Since then, Evo and Rufus have come to an "arrangement," where Rufus is taken care of and given free rein among the store's robopets and other toys, and Evo uses its presence as a successful promotional tool.

**Urania (Metasapient)**

On December 24th, 2070, the sky above New York was ablaze with new light shining from hundreds of high-resolution AR stars. The AI Urania had unveiled her newest art project to mankind as "a gift to celebrate the collaboration of man and machine." The digital starry sky was programmed over the course of two months by a collaboration of six digital design artists and two AIs under the leadership of Urania.

**Drone Pilot**

An AI with this quality likely evolved from a drone Pilot program and retained its abilities. The AI may "jump into" drones and control them like a rigger, using their rating in place of Pilot. The AI is also capable of loading, converting, and using drone autosofts. AI-driven drones use the attributes, skills, and Matrix Initiative of the AI.

Note that AIs with this quality are typically only skilled at operating a particular type of drone or device, and will be unfamiliar with other drones (at the gamemaster's discretion, apply a negative dice pool modifier or simply disallow it). See *Pilot Capabilities,* p. 103, *Arsenal.*

**Emulate**

AIs with this quality are able to emulate programs they need, similar to the threading of technomancers (p. 240, *SR4A*). Use the same rules as threading, except the AI uses Rating + Software, and the emulation process does not cause Fading.

**Improved Realignment**

AIs with this quality evolved more effective regeneration routines in their source code. For every interval of the Extended Healing Test, an additional box on the Condition Monitor is healed.

**Redundancy**

Essential algorithms, routines, and other program structures are multiplied in the core of the AI, making it harder to kill. The AI gets 2 additional boxes on its Matrix Condition Monitor.

**Rootkit**

Due to its innate understanding of Matrix coding, the AI is much more effective at hiding its presence within a node and can become nearly invisible to other Matrix users. Matrix Perception Tests against the AI suffer a –6 dice pool modifier.

**Sapper**

The AI has an intuitive sense for weaknesses in a Firewall or other defenses. It receives a +2 dice pool modifier on all Exploit Tests.

**Snooper**

The AI is more effective at accessing and correlating data that can be used to track another Matrix entity. It receives a –3 threshold modifier when making Track Tests.

**Spawn**

An AI with this quality is able to copy its programs and give them away to other Matrix users. Treat programs "spawned" in this way as illegal and unpatched program copies, in that they suffer from degradation over time (see p. 108). Spawned programs may be patched as normal.

An AI who possesses both this quality and the Emulate quality (p. 169) may spawn copies of emulated programs for others users as well. Spawned and emulated programs must still be sustained by the AI, as per normal threading rules.

Similarly, an AI with both Spawn and Emulate qualities may emulate agents for itself. Emulated agents may be loaded with

spawned or emulated programs. The number of agents that maybe spawned is limited to the AI's rating.

## NEGATIVE AI QUALITIES

Evolution is an imperfect process, and sometimes AIs evolve with mutations that hinder their development and survival. The gamemaster is encouraged to apply Negative qualities to AIs in order to limit their abilities, provide ways in which they can undermined, and to underscore the continually evolving landscape of the Matrix.

### Corruptor

AIs with the Corruptor defect suffered fundamental defects to their programming during their evolution. This means that the AI has an unfortunate tendency to trigger malfunctions in other programs with which it interacts. Treat this as if the AI has the Gremlins quality (p. 94, *SR4A*) at Rating 2. The gamemaster should also make use of this Negative quality for dramatic effect as best suits the story.

### Fragmentation

During its birth, the AI's core programming was fractured and failed to fully merge again properly, or a core element to its programming was somehow deleted or lost. In effect, this creates fundamental flaws in the AI's "personality." Swarm AIs suffer from effects best compared to mental illnesses like schizophrenia or paranoia, which makes their behavior unpredictable. The gamemaster should choose an appropriate mental defect for the AI, one that both makes its character unique and hampers its functioning (perhaps considering the Negative mental qualities given on pp. 163-164, *Augmentation*). At the gamemaster's discretion, this quality may inflict negative dice pool modifiers to certain tests, especially social interactions.

### Real World Naivete

As creatures of the Matrix, most AIs are at best ignorant of the functionings and goings-on of the physical world—some AIs have never even heard of it or simply refuse to believe it exists. Even if their original programming involved interaction with the physical world in some way, they may not fully grasp the entirety of meatspace or minor things like gravity and other physical laws. As a result, AIs with this quality have little knowledge of the real world and may suffer hefty negative dice pool modifiers (at the gamemaster's discretion) when interacting with it or otherwise exercising knowledge about it.

## GHOSTS IN THE MACHINE

Ever since the Crash 2.0, numerous rumors and stories have circulated the Matrix of alleged sightings and interactions with people in the Matrix who were long dead in the physical world—to date, however, none have been verified. Some tales describe a Matrix user spotting the persona icon once used by a dead friend, relative, or lover, followed by a strange interaction that implied the encounter was not simply the user's imagination or someone's idea of a bad joke. Other reports tell of strange, flickering icons that repeatedly appear in the same (sometimes restricted) nodes, repetitively performing the same actions, but that are unresponsive and mysteriously vanish when confronted. Still others whisper of poor victims who are mercilessly pursued online by stalkers who claim to be someone that is dead, tormenting and harassing them with creepy calls and messages, and occasionally tracking their affairs and interfering in their life. A few claim to have been attacked by these strange *e-ghosts,* an experience compared to a Black IC attack or worse. A few mysterious deaths hint that some of these encounters may be fatal.

E-ghosts, also called ghosts in the machine, are very rare digital entities possessing the memories and personalities of people who died online during the Crash 2.0. It is unclear what causes these e-ghosts to manifest. Some theorize that these are merely AIs, created during the Crash, that were somehow imprinted with the mental state of a Crash victim. One author has suggested that these aren't ghosts at all, but simply some sort of new program designed to emulate people based on the long datatrail of their life's interaction with the Matrix. Others postulate that some sort of rogue program—a side effect of the Jormungand worm, perhaps—managed to upload the brains of people who were trapped and killed online, giving them eternal life as some sort of autonomous program. Still others point their fingers at technomancer trickery, or wonder if these are in fact ghosts of the spiritual sort, somehow trapped within the machine. The truth is that no one knows, and no one can even say with certainty if these are truly the ghosts of the dead, living on in the Matrix, or something else entirely.

### Echoes from the Digital Realm

In terms of rules, e-ghosts are handled like AIs, which means that they have their own Mental attributes and skills, but also some unique abilities. The "programs" they carry are ingrained abilities that help them to navigate the Matrix. E-ghosts have ratings from 1 to 6 to reflect their power.

The important part to consider when crafting an e-ghost is deciding how good a copy it is of the dead character (note that copy quality is a separate factor, not dependant on the e-ghost's rating). Most e-ghosts tend to be far from perfect copies. They may have only some or none of the character's memories, and certain facets of the character's personality may simply be missing. At best, an e-ghost is likely only to have a faint recollection of their previous life. The memories most constantly retained are the events leading up to death, unfinished tasks, and major grievances. Some e-ghosts are such poor emulations that they have only occasional flashes of their former life, wandering confused and enraged through the Matrix. Others are unaware of their demise, believing themselves to still be alive, but somehow trapped online. A few are quite cognizant of their status, but do their best to interact with Matrix users and establish networks that grant them influence in the real world.

The stats given here for e-ghosts are simply a recommendation; gamemasters should tailor the e-ghost's skills, programs, and qualities as fit the story.

**E-Ghosts**

| CHA | INT | LOG | WIL | EDG | Matrix INIT | IP |
|---|---|---|---|---|---|---|
| R | R + 1 | R | R + 2 | R – 2 | INT + Response | 3 |

**Skills:** Computer (R), Cybercombat (R), Hacking (R), additional skills as appropriate to the character

**Programs:** Analyze (R), Blackout (R), Browse (R), Command (R), Edit (R), Exploit (R), Reality Filter (R), Stealth (R), Track (R)

**Qualities:** Code Flux, Corruptor, Fragmentation, Redundancy, Rootkit

## UV NODES—AT THE EDGE OF REALITY

In hacker nodes across the world, starry-eyed icons listen awestruck to tales of encounters with the holy grail of system sculpting: ultraviolet nodes. Ultraviolet (UV) nodes are legendary locales where the processing power, data capacity, simsense output, and sensorial rendering is so concentrated that the VR resolution advances beyond realistic and high-definition and into the hyper-real. Accessing a UV node is an experience unlike any other in the Matrix—more akin to entering an alternate reality than immersing yourself in VR.

The resources and skills to craft a node of this potency are rare and far between, and are reserved for critical and secretive projects behind deadly corporate firewalls, far from prying eyes. Only a few dozen such nodes are rumoured to exist, and typically they require much effort to maintain. Rumors persist, however, of spontaneously appearing UV nodes in certain high-density information-management systems, or of UV nodes somehow crafted by the likes of AIs as personal domains.

The hyper-reality of UV nodes is not without its danger—yet another reason they are hidden from the public. They are valuable for their ability to simulate realistic and flexible conditions, especially environments that might normally be hazardous to metahuman life.

### UV Node Requirements

The construction of a UV node requires state-of-the-art components and software with dedicated support systems, and is no light undertaking. The minimum Response and System ratings needed is 10, representing a pinnacle of processing ability and an OS customized and optimized for high-resolution graphic displays, physics, and other details of a realistic virtual environment.

To fully experience a UV node, a user must be running with hot sim. Accessing such a node with AR or cold sim VR is underwhelming, and simply misses out on the node's potential (similar to a normal node in these regards). Many UV nodes, however, are configured to block AR and cold sim users.

### Beyond Reality

The metaphor enforced by a UV system is overwhelming—reality filters automatically fail, and all iconography is automagically converted to fit. When a UV node is accessed, the simsense signal is automatically amplified, elevating the virtual environment to the point where it seems more real than reality. Persona icons are usually discarded; instead, users typically appear as their normal selves (a sim reading of their personal mental image), adapted to fit the node's metaphor. Software, complex forms, and even echoes are also converted, taking on the appearance of gear appropriate to the environment. Agents, sprites, AIs, and e-ghosts are translated as devices or creatures fitting the metaphor.

Due to the hyper-real nature of UV nodes, characters use their physical skills and abilities as if they were acting in the real world. If a character's Attack program appears as a handgun in the node, for example, he may fire it using Agility + Pistols rather than Cybercombat + Attack. At the gamemaster's discretion, some software may provide the character with skills he doesn't normally possess (Stealth providing Infiltration or Shadowing skill, for example). This allows the gamemaster to run the UV node as if the characters were in physical reality. Characters may still perform Matrix actions, but when possible these should be interpreted as "physical" actions. Magic, of course, does not function in UV nodes.

As a result of a UV node's potent sim signals, damage dealt within the node is applied directly to a character's Stun or Physical Condition Monitor in the form of dangerous biofeedback, similar to that inflicted by Black IC.

It is rumoured that some UV nodes possess the capability to alter subjective time, slowing it down or speeding it up, so that an hour spent in a UV node could seem like 10 hours or 10 minutes.

### Back to Reality

Due to the overpowering simsense connection that UV nodes require, it is next to impossible to block the sim signal out and sense, move, or react to the physical world. Even attempting to do so is difficult, requiring a Willpower + Logic (4) Test, and even then the modifier to meatspace actions is –8 rather than the usual –6.

For the same reason, dumpshock suffered when accessing a UV node is stronger than usual, inflicting 8P damage and doubling the duration of disorientation.

### UV Addiction

The simsense signal transmitted by a UV node is equivalent in strength—and addictive potential—to a BTL sim. Every time a user logs off from the UV node, roll an Addiction Test (p. 256, *SR4A*) to determine if they have picked up a habit. Addiction to a UV node is the same as BTL addiction—a character who can't get one can satisfy their fix the other way.

Note that UV nodes are not just addictive to metahumans—AIs, e-ghosts, and even sprites can become addicted to a UV node. In their case, the addiction is in part due to the peak simsense signals, and in part to the feeling of freedom and power provided by a UV node's high system ratings.

### E-GHOST CULTS

Along with the reports of e-ghosts circulating the Matrix are more subdued whispers of cults whose seek the special sort of immortal status that e-ghosts have obtained. Some of these cults promise to lead their followers to immortality if the users obey their orders. Others have formed to serve existing e-ghosts, in the hope that their service will be rewarded. One such rumored cult is the Moebius Cluster, allegedly comprised of scientists from various fields and led by an e-ghost named Neurosis, who are researching self-motivational robotic units. Another rumor tells of a Matrix wetwork ring called Last Byte, led by an e-ghost called Nergal who appears on numerous police wanted lists around the world. According to whispered stories, Nergal's trademark is to convert his victims' bodyguards into assassins, and then leave them to take the fall.

Urgent Message...

### RUMORED UV NODES

A UV node's existence is often a tightly-kept secret, but several rumors of such places permeate the shadows. Here are a few examples:

**Ares Firewatch Combat Simulator**

Recognizing the potential of programmed VR worlds for combat training, Ares has ramped up the capabilities of their elite Firewatch units' training simulator to provide an experience that is just as frightening, chaotic, painful, and dangerous as real life combat. Firewatch personnel are trained in a wide variety of environments and situations, from bug hunts and conflicts with dragons to desert warfare and zero-g space scenarios.

**Cataclysm Generator**

This secret project, operated by the megacorp Proteus, researches the behaviour of metahumans when they are confronted with massive disasters and apocalyptic scenarios. To achieve realistic results, test subjects are kidnapped or lured in under the pretext of other projects and inserted unwittingly into the system without preparation. After the test series, the subjects are administered a chemical cocktail that erases their memories of the experiments and released.

**Flesh Trade**

This illegal node, rumoured to be operated by a consortium of Triad groups, sells itself as an out-of-this-world sex experience. Part brothel and part sex party, the Trade also offers an assortment of BTL feeds, and for a premium sells customized experiences, where you can bring any sort of deviant fantasy to life. Aside from the desire to hook their customers on BTL, the real business of the node lies in secret psychotropic subroutines they also run on their clients.

**The Nexus**

The world's premier data haven, the Nexus serves as a mirror site for numerous shadow Matrix nodes, social networks, and archives. Hidden away in Denver, this site managed to survive the Crash 2.0 almost unscathed, and remains a crucial resource for shadowrunners and info brokers. Its data depositories have grown so massive that its core nexi now require massive levels of processing power just to manage all of the data, even in an era where data storage is cheap.

## RESONANCE WELLS

Resonance wells are nodes within the Matrix that hum in Resonance. While these places are often unremarkable to normal Matrix users, technomancers experience them as hyper-real nodes—similar to UV nodes (p. 171)—that almost feel alive, resonating with the energy of the Matrix. It is unclear how resonance wells are created, and no technomancer has yet found a way to create a resonance well, even with any kind of digital feng shui or geomancing ... although *many* have tried. Some have speculated that these places are actually wormholes or gates into the resonance realms from which excess Resonance leaks into the Matrix. Others hold wild sprites (or sprites in general) responsible. The truth is, nobody knows.

A number of resonance wells that were known before Crash 2.0 and used by the otaku to achieve submersion were destroyed, dried up, or shifted location. The appearance of a new resonance well does not follow a certain scheme; they could potentially form anywhere, though there have been no reports of a resonance well in a major public node—they seem to manifest only in the quiet and unvisited corners of the Matrix. Resonance wells are mostly permanent (albeit *exceptionally* rare) and stable as long as the node does not shut down—crashing the node kills the resonance well in most cases. They can also, rarely, appear temporarily (a phenomenon known as a *resonance flash*) or migrate through different nodes in repeating cycles (*resonance undulations*).

Due to their positive effects on Resonance abilities, resonance wells are sought out by technomancers, guilds, and free sprites alike, and are heavily contested (comparable to power sites and mana nexi in the Awakened world).

In game terms, a resonance well has a rating that represents its power. This rating acts as a positive dice pool modifier for all tests that involve Resonance, whether made by a technomancer or sprite: Fading Tests, Compiling and Registering Tests, uses of complex forms, and so on.

Dissonant technomancers (see p. 175) suffer the opposite effect of regular technomancers when they encounter a resonance well: they suffer a negative dice pool modifier equal to the well's rating. Dissonance variants of resonance wells, called *dissonance pools,* also exist. These pools have the same impairing effects on technomancers as resonance wells have on dissonants.

### Resonance Rifts

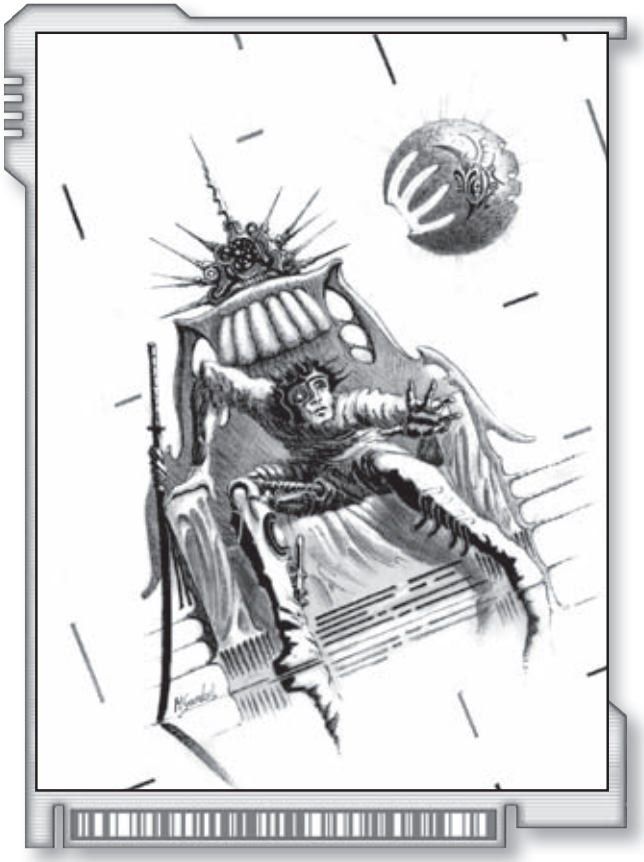
A few resonance wells are known to inexplicably act as gateways to the resonance realms (usually a specific resonance realm), transporting unwary users against their will. These *rifts* are uncommon, tend to occur without warning, and do not last for long. If stable rifts exist, they are not talked about openly, and are likely cherished and protected.

Such rifts provide an open passage for non-submerged technomancers to access the resonance realms, even allowing the travellers to bypass the Event Horizon (see p. 174). In fact, rifts may pull in unwary or unwilling Matrix denizens who have the misfortune of coming across one—a successful Willpower + Charisma (3) Test is necessary to avoid being sucked in.

While most resonance wells are invisible to non-technomancers, resonance rifts tend to (but not always) take more visible forms, usually demarked with iconography such as swirling vortices, tornadoes of data, or ugly pixelation and de-rezzed stains bleeding across a system's sculpted environment.

## RESONANCE REALMS

There is a certain feeling that every technomancer knows when diving through the Matrix. It's more than the constant buzz of data traffic in the background, it's the feeling that there



is something *larger* beyond the curtain of icons and background processes. Or perhaps it's a feeling that there are massive depths lying beneath the surface of the Matrix, unexplored and unseen places from which Resonance seeps into the virtual realm. From the otaku before them, some technomancers have learned to access these levels beyond. On the other side, they discovered unique places, thriving with sprites, lit from within by abundant Resonance that shone as bright as the sun. These places are called *resonance realms.*

Technomancers today are still learning about these realms, exploring their depths, discovering new ones, conversing with their denizens, and learning new things about themselves in the process. Corporations and researchers also strive to learn what they can, debating and testing the nature of the places. Some think these realms form some sort of higher-order structure within the Matrix topology, while others theorize that these realms do not normally exist, and instead are formed when a technomancer enters and dissolved when he leaves. A few avant-garde theories even suggest that these realms are actually some sort of magical metaplane, though these are widely derided by technomancers and thamauturgists alike.

Much like the metaplanes, no detailed map of the resonance realms exists, and in fact getting even two technomancers to agree on the topography, purpose, and appearance of a particular realm can be a challenge. Some sprites talk as if they have a "home" resonance realm of sorts, and some technomancers believe that their paragons maintain their own distinct realms as well. Still other realms have their own strange and sometimes inexplicable purposes, and may even change drastically from one visitation to the next.

### Diving into the Depths

Only technomancers who have undergone submersion (p. 243, *SR4A*) are able to create a connection to the resonance realms (though sprites move freely between the realms and the Matrix). Accessing the resonance realms is no easy task, however, requiring the technomancer to break through the Event Horizon (see p. 174). Non-technomancers may only access the resonance realms via a resonance rift (p. 172) or with the help of a free sprite (p. 157).

The sensorium of the resonance realms ranges from abstract obviously digital worlds to extremely realistic UV-like environments. The iconography typically subscribes to a metaphor that is in line with the node's apparent purpose or denizens, though the look and feel of these places have been known to change, sometimes quite quickly and drastically.

In game terms, resonance realms may be handled as any sort of Matrix node, or the gamemaster may apply the rules for UV nodes (p. 171) and treat visitors as if they were acting in a physical space. Visitors who suffer damage in the resonance realms manifest such damage on their physical forms. Characters who die in the resonance realms enter a vegetative coma from which they never awaken.

Breaking through the Event Horizon brings about major changes to the Living Persona and the technomancer's Matrix connection. There is no recognizable data trail between the technomancer and the resonance realm, and the technomancer's body remains in a vegetative state, unable to interact with his environment, as long as he is in contact with the resonance realm.

Subjective time in the resonance realms almost always differs from real-world time, so that a trip that seems to last for 10 hours may in reality have taken only 10 minutes or, more drastically, 10 days. Some technomancers have been caught off-guard by this difference, their physical bodies nearly dying from dehydration or other factors while their minds were away.

**RESONANCE REALM:**
*The Endless Archive*

Every single bit of data leaves indelible trails in the Matrix. With every new piece of generated, transferred, or deleted data, the fragments of the old data are buried beneath the newcomers and will soon thereafter be nearly unreachable for any user who searches for them. These fragments sink deeper and deeper into the background of the Matrix, coming to rest in the storage banks of the Endless Archive. Technomancers who have explored this realm tell of tall, dark halls lined with endless bookshelves, containing untold amounts of unsorted data that dates back to the invention of computational devices. The corridors between these bookshelves are sometimes occupied by sprites that sift through the data like some sort of obsessed librarian, but who do not sort it in any way that is understandable to metahuman minds. Some of these sprites are willing to search for archived data—data long lost and irretrievable in the Matrix—but usually only in exchange for data that has never appeared in the Matrix.

## RESONANCE REALM SEARCHES

Technomancers (and others) who visit the resonance realms have the opportunity to work wonders they would never be able to do in the normal Matrix. The resonance realms offer certain tricks and shortcuts that might allow a character to ignore fundamental rules of Matrix topology, bypass system security, or acquire inaccessible data. To make use of these hacks, however, the technomancer must find the proper path through the resonance realms, a process known as a *resonance realm search.* This is the true challenge when visiting a resonance realm.

### Harmonizing with the Resonance

Accessing the resonance realms is no easy matter. Before a technomancer even begins his search, he should take care of his physical security. Trips to the resonance realms may take extensive amounts of time, so it is always a good idea to choose a safe place for your body or at least leave it in the care of good friends.

To start a resonance realm search, a technomancer must clear his thoughts, cut off all active connections and subscriptions, and immerse himself in the virtual reality of the Matrix. By concentrating on the constant background noise, harmonizing with its frequencies, a submerged technomancer can trace the streams of Resonance back to their source—the resonance realms. This requires a Resonance + Fading attribute + submersion grade (12, 1 hour) Extended Test. Once a technomancer has located this backdoor, he can begin his journey to the resonance realms—but he must first pass the Event Horizon (p. 174).

**RESONANCE REALM:**
*The Shattered Haven*

The first technomancers to enter the resonance realms had heard from the otaku before them of a fantastic digital city that arose from a vast river of data, a place known as a sanctuary for visitors needing respite from the resonance realm wilds. What they found was not what they expected. The formerly proud city of Haven was ruined and ablaze, its resident sprites engaged in an ongoing civil war against their dissonant brethren. The flow of information around the digital spires was corrupted, dark and oily with malignant data.

The sprites living in this place are willing to share any knowledge they have that might be of use in combating dissonance. As their digital structures slowly succumb to entropy, they may seem to be fighting a hopeless war, but they refuse to give up. The entropic sprites they war against fully expect to claim this place as their own, but they may also be willing to deal with outsiders, especially if it furthers their own goals.

At the gamemaster's discretion, this initial effort of finding a backdoor to the resonance realms may require the technomancer to access a node (or nodes) that he doesn't have permission to enter. This may particularly be the case if the technomancer is seeking the path to a particular resonance realm. Alternately, the trail may take the technomancer to a resonance well, suggesting some possible linkage between the wells and realms. Each resonance realm search takes the technomancer by a different path. Some technomancers claim to have accessed the resonance realms merely by immersing themselves in the VR of a single, isolated node that was disconnected from the rest of the Matrix.

### Event Horizon

Every time a technomancer enters a backdoor to the resonance realms, he must first cross the Event Horizon. The appearance of the Event Horizon changes based on the stream of the technomancer, but it invariably appears as some sort of barrier or obstacle that hinders his progress to the realms. Some call this the Great Firewall, carefully guarding access to the realms, whereas others consider it to be the Cipher, an intricate puzzle or code that can only be solved with the proper key.

Whatever its true nature, the Event Horizon forces the technomancer to come face-to-face with his own secrets, weaknesses, and insecurities. Not only does the Event Horizon have access to any information that has ever appeared on the Matrix, but it also seems to tap into the technomancer's own memories and subconscious. This procedure may range from a review of the digital records that testify to how the technomancer failed to help a friend in need to forcing the technomancer to experience the sensorium of someone he has killed. The purpose of this test seems to be a review of the technomancer's "programming," to root out bugs, bad code, and security flaws. In most cases, it is a wrenching emotional experience. If the character cannot get through the experience, then their journey stops here.

If two or more submerged technomancers undertake a resonance realm search together, they are privy to the experience through which each of the others goes.

### Navigating the Realms

Every resonance realm search can be broken down into a series of tasks that the technomancer must complete in order to achieve his goal. The gamemaster determines the number and scope of these tasks, but they should be weighted in accordance with the severity of the goal. Typically these tasks relate to the goal and the resonance realm(s) being visited. For example, a search to erase data (see p. 175) could require the technomancer to track down all instances of that data, represented as fruit, hidden away in an expansive digital forest. Likewise, a technomancer hoping to acquire a powerful free sprite's source code should face numerous obstacles and challenges the sprite has placed before him. As a general guideline, the rating of whatever is the target of the search can be used to determine the number of tasks to be completed.

### Goals

The goal of a resonance realm search may differ from technomancer to technomancer, but the following goals are the most common. For developing additional goals, gamemaster can use these as a guideline.

**Enforce a Resonance Bond:** A technomancer who possesses a free sprite's source code and wishes to force that free sprite to enter into a resonance bond (see p. 160) may travel to

the realm where the source code was found in order to compel the sprite to create the bond. If the technomancer does not wish to anger the sprite, he can instead engage in this search in order to unveil something the sprite wants or needs, so that he may acquire it and use it bargain for the resonance bond.

**Erase Data:** Sometimes the goal is not to find information, but to destroy it. Though this goal is much harder to accomplish, a technomancer may seek to erase a piece of data permanently from the Matrix. If successful, the data is eliminated or corrupted beyond repair, no matter how securely it is protected by encryption, firewalls, or other means (non-Matrix information, such as hardcopy or personal memories, remain unaffected). Technomancers are wise to take note, however, that while this action may remove such information from the Matrix, it is hinted that the Resonance never forgets, and that such data may be retrieved through an Recover Data resonance realm search—albeit one made much more difficult by this action.

**Find Data:** A technomancer who knows that a certain piece of data exists, but doesn't know where to find it, can ask the Resonance itself. The gamemaster determines how hard the data's location is to find, based on its real world availability. This search will not necessarily leave the technomancer with the data in hand, but it will tell the technomancer where to seek it. This search may also be used to find or trace a data trail, specifically one that was routed through the resonance realms.

**Find Sprite Source Code:** If a technomancer wants to register, track, or decompile a free sprite (see p. 157), or recover a registered sprite that has been disrupted (p. 159), he must first find the sprite's source code.

**Glitch a Node:** A technomancer can weaken the defenses of a node in preparation for a hack, or simply seek to disrupt the node and create complications. In this case, he can undertake a resonance realm search to find a way to glitch the node. If successful, Resonance turbulence disturbs the node for Resonance x 2 hours. The effects of this disturbance is up to the gamemaster, but may include a dice pool modifier for all actions made by the node and its defences, unexplained software crashes, corrupted data, weakened Signal, and a scrambling of access privileges that requires users to make tests for Matrix actions that they would normally perform automatically.

**RESONANCE REALM:**
*The Great Connection*

Embedded deep within the resonance realms is a giant tree whose roots are hidden in a lake of data: The Great Connection. This realm is said to link to every node in the Matrix, no matter how isolated or secure. Each leaf reflects a node, with newly connected nodes represented as sprouts, active nodes as fully-grown leaves, and the leaves of disconnected nodes withering and blowing away in the wind. The air is full of pollen, reflecting the constant flow of data traffiic. Sprites in the form of birds, bees, squirrels, and other animals crawl the branches.

**Hide a Data Trail:** A technomancer can undertake a resonance realm search to find a way to hide his data trail. If successful, the technomancer's data trail through the Matrix after completing this goal is inexplicably routed through the resonance realms for Resonance x 2 hours. Anyone that attempts to track the technomancer's data trail from that period will find that it simply disappears without explanation, as if washed away by pure Resonance. Submerged technomancers may ascertain that such a trail has been hidden, and may attempt to follow it with a resonance realm search of their own (see *Find Data,* above).

**Learn an Echo:** A technomancer seeking to learn a new echo can undertake a resonance realm search to discover how the echo works. The technomancer must spend Karma just as he would if he learned the echo from a teacher or a free sprite (see *Learning Echoes,* p. 145).

**Recover Data:** Every piece of data in the Matrix generates an echo in the Resonance, meaning that it is possible to still find such data long after it has been deleted from the Matrix. The difficulty of finding such erased information depends on how old and scarce it was. Only data that existed at some point on the Matrix since the Crash is certain to be found, though some technomancers suggest that any data that has ever existed on a computer network or electronic device may be found by visiting the Endless Archive (p. 173).

**Submersion Task:** A technomancer undergoing submersion may complete a resonance realm search in order to lower the cost of the submersion (see p. 141).

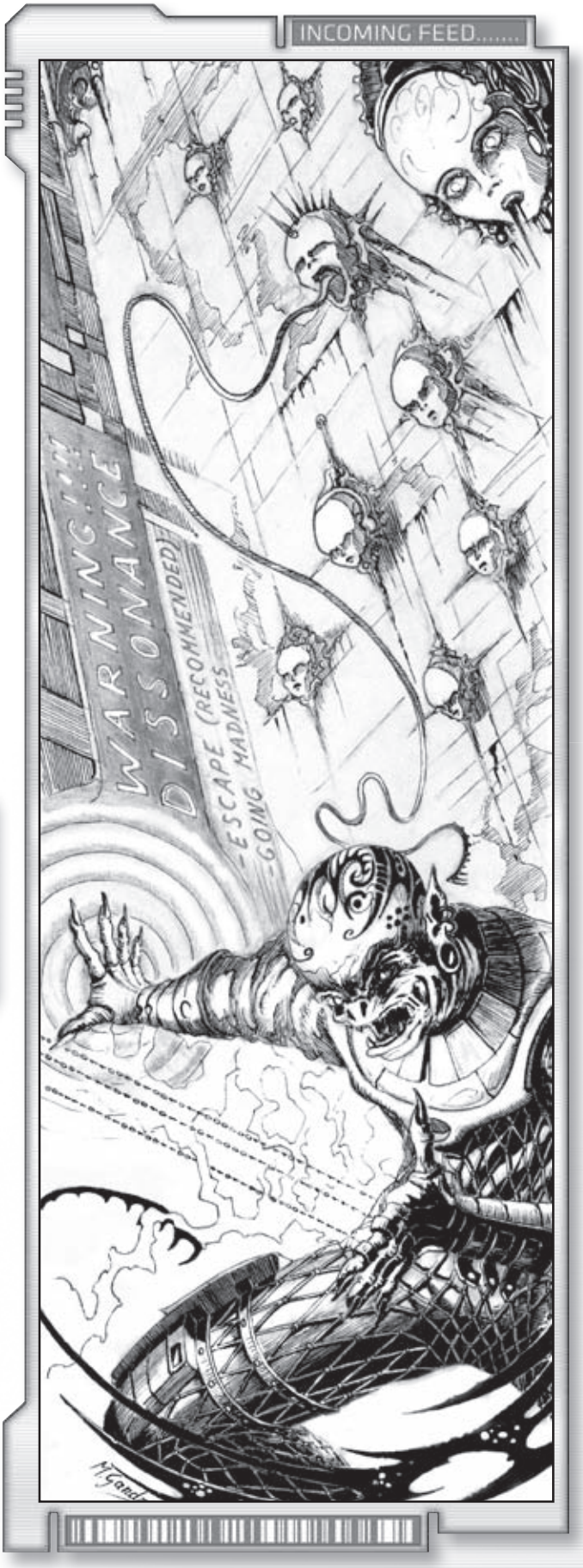
## DISSONANCE

Dissonant technomancers are Emerged individuals whose sanity and Resonance have been corrupted or warped by some sort of neurological or mental disorder or anomalous phenomenon. Whether this is caused by the oft-speculated mutation in the technomancer genes, biochemical or neurological instability, cerebral damage, neuro-degeneration (for instance, due to cancer, neural diseases, or viral infection), or some purely psychological phenomenon brought on by interaction with the Matrix is still unknown.

While most technomancer streams emphasize the harmony of the digital world, revere the clarity and immaculateness of its code, and embrace the endless horizons and possibilities of a virtual world, dissonant technomancers are driven by warped ideas and irrational or even insane thinking. They revel in digital chaos and absurdism. Even worse, they seek to infect the Matrix with their digital blight, spreading fractal code, the hallmark of the Dissonance.

### Disharmony and Madness

Dissonants follow an antithetical concept of the Matrix that only few dare to grasp. Dissonance itself was a new phenomenon some decades ago, spearheaded by a dissonant otaku known as Pax (probably the first one warped by her own psychopathic behavior). Her unleashing of a dissonant worm construct named Jormungand was one of the factors leading to the Crash 2.0. With the recent Emergence of technomancers and sprites, it has become clear that the Dissonance did not disappear with Crash 2.0, but rather has become more prominent than ever.




Dissonants are united by their different breeds of cyberpsychopathy, a condition that is usually characterized by lack of conscience, poor impulse control, and manipulative behavior, expressed primarily online. Although some dissonants also show psychopathic and antisocial behaviors in real life, there have been reports of dissonant technomancers that exhibit a different demeanor when subjected to static or dead zones—as if they have been treated with anti-psychotic drugs such as tranquilizers or neuroleptics. As current theory goes, it seems that the interaction of the technomancer's unique neurophysiology and bioelectrics with the Matrix is the cause of the phenomenon.

Since the particulars of dissonants are tied to their personal cyberpsychopathic disorder, they develop their own unique ways to wield Resonance. As such, dissonant technomancers still follow the basic rules of technomancers and streams (see p.136 and p. 239, *SR4A*), but each dissonant technomancer pursues his own antithetical belief and thus follows a unique Dissonance stream that that fits his agenda.

Although no credible reports exist of any technomancer surviving one, dissonance realms appear to exist.

## DISSONANT STREAMS

Due to their corruption, dissonants are consumed by their distorted perception of the Matrix and twisted philosophies of the code. Although each dissonant is unique in his delusion, they often form alliances with each other to perform "higher" goals that fuel their agendas. The sample dissonant agendas that follow are simply the most common encountered so far.

The attribute used for Fading and the sprites each dissonant stream may compile are left up to the gamemaster—to keep the players guessing.

### Cyberdarwinists

Cyberdarwinists view the majority of metahumanity as too weak or unfit for the evolutionary challenges of the modern world. To save it from its own downfall, mankind must be securely controlled by a superior machine intelligence that makes decisions for their own good. Cyberdarwinists see Dissonance as the key element in creating this one large, self-improving, artificial general intelligence, raised through the dissonant evolution of the Matrix. They are trying to bring about this intelligence by redesigning and reprogramming the source code of the Matrix and transforming all resonance realms into dissonance realms. Totally devoted to their cause, most Cyberdarwinists are utterly fanatic.

### Discordians

Named after the Roman goddess of strife, Discordians view themselves in a fraternal struggle with their brethren (technomancers that follow the streams of the Resonance) whom they call *Cainites* (traitors to blood relatives, after the biblical Caine). Determined to eradicate the Cainites or persuade them to convert, the Discordians wage a genocidal conflict not only in the Matrix but in the real world as well. They seek to shatter technomancer associations or to kill any individuals who have "come out" as technomancers.

### Infektors

The Infektors' ultimate goal is to recreate a "dark Matrix" formed from Dissonance. As virtual plague bearers, they seek to contaminate nodes, turning them into dissonance pools, or to infect data with viral dissonant code by the mass spawning of Contagion sprites.

### Nytemares

Surpassing even the vilest Matrix pranksters, these dissonant technomancers revel in digital flagrancy and virtual abomination, seeking to create a nightmarish version of cyberspace. While the less direct nytemares "only" hack the iconography of commonly-frequented nodes into grotesque metaphors in order to bask in the horror of those who face it (or become trapped in it), their more actively involved counterparts prey upon and torment easier targets. Stalking these targets (often in real life in addition to virtually), they try to discover their greatest fears. They then seek to confront their targets virtually with these fears, in an effort to torture them, break them, push them over the edge, or drive them insane.

### The Sublime

The Sublime are dissonant supremacists. Feeling themselves exalted and superior to normal Matrix users, they view non-Emerged and often even normal technomancers as relics who will never achieve true status in the Matrix, treating them as servants, slaves, or even cattle. The Sublime tend to enslave and torture Matrix users with their complex forms or in dissonant virtual machines just for their own satisfaction.

## DISSONANT PARAGONS

Though the concept of virtual emanations in the Matrix is not even widely accepted among philosophers, psychologists, and Matrix experts, dissonant technomancers that have been captured and interrogated by KivaNet have spoken of distorted entities to which they have sworn allegiance.

The following dissonant paragons are examples of corrupted templates and archetypes that have their roots in the Dissonance phenomenon.

### Abort

Abort is the personification of the "blue screen of death," the embodiment of all bugs and software errors that accumulate within cyberspace. Thrilled by the failure of code due to errors, dissonant technomancers following Abort like to install software errors in existing software and crash nodes just for the fun of watching the iconography go down the drain.

**Advantages:** +2 dice to all Crash Tests, +1 die for dissonant Crack or Fault sprites (choose one)

**Disadvantages:** An Abort technomancer must make a Willpower + Charisma (3) Test to take any other action in cybercombat except for trying to crash his opponent's software.

### Disinformation

Disinformation is the embodiment of the deliberate dissemination of false information spread via the Matrix in form of forged media, malicious rumor-mongering, and fabricated intelligence. Disinformation technomancers seek to mass-manipulate audiences and Matrix users via Matrix trolling, viral marketing, and memetic warfare.

**Advantages:** +1 die to all test with skills from the Influence skill group, +1 die for dissonant Data or Tutor sprites (choose one)

**Disadvantages:** Disinformants must succeed in a Willpower + Charisma (3) Test to pass truthful, complete, or non-doctored information via the Matrix to non-dissonant technomancers.

### Jormungand

Jormungand, the world-serpent that poisons the Earth before the Final Battle of Ragnarök, is both an embodiment of the ultimate weapon of mass destruction, and the personification of dissonant Matrix malware (as per the Jormungand worm's role in the Crash 2.0). Those dissonant technomancers who follow this paragon revel in the corruption and permanent destruction of code and information in the Matrix.

**Advantages:** +2 dice Corrupt Tests, +1 die for dissonant Data or Code Sprites (choose one)

**Disadvantages:** Jormungand technomancers are destructive and will take every opportunity to devastate a node by permanently deleting or corrupting its data. They must succeed in a Willpower + Logic (3) Test to leave a node they have hacked into unscathed.

### Nemesis

Interpreted in its original meaning ("to give what is due"), Nemesis is the remorseless personified digital fate and retribution. While some follow her as the embodiment of an avenging angel and a paragon that punishes those deemed unworthy in the name of the Dissonance, some see her as the true instigator of Crash 2.0 and the Dissonance worm, calling Nemesis by her old Roman name, Pax-Nemesis.

**Advantages:** +2 dice to Con Tests, +1 die for dissonant Fault or Sleuth sprites (choose one)

**Disadvantages:** A Nemesis technomancer must make a Willpower + Charisma (3) Test to restrain himself from punishing those whom he feels deserve it.

### Noise

Noise embodies the defilement of signal and code. Though the term is sometimes used as a synonym for Resonance, Noise technomancers celebrate the corruption of resonant code (signal) into dissonant code (noise) and view Noise as the fundamental digital force that pervades everything, albeit on an as-yet nearly unrecognizable level. By spreading Noise, technomancers seek to jam the channels of Resonance, instead filling the Matrix with the discordant hiss of Dissonance.

**Advantages:** +2 dice to Threading Tests, +1 die for dissonant Courier or Code sprites (choose one)

**Disadvantages:** Noise technomancers rely on the buzz of Matrix more so than others, and suffer double the modifiers applied to Matrix and non-Matrix actions when caught in static or dead zones (see p. 220, *SR4A*).

### Snuff

Snuff is the incarnation of electronic perversion, regardless of format. Snuff is only stimulated by the most abhorrent crimes (rape, murder, metahuman sacrifice, pornographic perversions,

etc.) perpetrated by means of media or simsense recordings for the purpose of entertainment. Since Snuff likes to watch, dissonant technomancers following Snuff revel in the abyss of the metahuman soul, and often become actively involved in following, observing, or even selecting later snuff victims, watching them through cameras and electronic sensors before going in for the kill.

**Advantages:** +2 dice to all Sniffer Tests, +1 die for dissonant Crack or Sleuth sprites (choose one)

**Disadvantages:** Snuff technomancer suffer a –2 dice pool modifier to resisting addiction to BTL or Matrix media.

### Tiamat

Tiamat is the monstrous embodiment of primordial chaos. Dissonants following this incarnation of chaos and disorganization view the Matrix as a flawed creation destined to be imprinted with a new order. Dissonance is seen as the seed of chaos that will wash over the digital realm to reshape the Matrix in a digital war. Technomancers following Tiamat consider themselves to be warriors of chaos, fighting a divine crusade against those who follow the Resonance.

**Advantages:** +2 dice to Cybercombat, +1 die for dissonant Crack or Tank sprites (choose one)

**Disadvantages:** –1 die to all Hacking Tests

## DISSONANT ABILITIES

Dissonant technomancers have access to techniques that no sane technomancer would ever touch.

### Node Mine (Dissonant Complex Form)

Node mines are dissonant versions of the Data Bomb program. Unlike data bombs, which are tied to certain files or data, node mines are attached to a "geographic" location within a node (actually a memory cluster dedicated to a portion of virtual space).

In game terms, node mines are treated as an area effect Data Bomb program that can be loaded with an Analyze complex form (similar to how agents load programs). The node mine is programmed to detonate either upon a certain time or when the Analyze complex form detects a particular target of choice (technomancer, sprite, hacker, etc.). Similar to patrolling IC, node mines with Analyze programs are in a constant probing mode. Node mines may also be equipped with program options available to Data Bombs, such as Black IC or Pavlov.

Treat a node mine attack as an area attack to all icons in the node with a DV equal to its rating. Gamemasters may choose to make these mines even nastier by associating further program options like Armor Piercing or Psychotropic with node mines.

### Dissonant Viruses (Dissonant Program Option)

In contrast to technomancers, dissonants can create viruses (p. 120) that can be installed into normal programs. Whether these possess the virulence to infect technomancer complex forms is left to the gamemaster. Gamemasters are encouraged to choose the abilities and effects of these dissonant viruses as they deem fit.

### DISSONANT DISEASES

The following dissonant diseases have been identified thus far:

**The Black Shakes**
**Vector:** Contact
**Speed:** see description
**Penetration:** 0
**Power:** 5
**Effect:** Tremor

Similar to those of TLE-x (p. 132, *Augmentation*), symptoms of the Black Shakes do not manifest immediately but rather develop over time, during which the pryon damages neurological pathways. Each month after infection, the gamemaster may require the Black Shakes victim to make a Body + Willpower (2) Test. If the test fails for the first time, the disease kicks in and the character starts to develop unintentional muscle contractions involving one or more areas of the body (hands, arms, head, face, vocal cords, trunk, or legs)—the so called "shakes." This inflicts a –1 dice pool modifier for all tests that involve Physical attributes at first. The tremors escalate after each failed test to a maximum negative modifier of –4. AEXD has proven to be ineffective against the Black Shakes, though brain surgery (see *Augmentation*) can reset the symptoms.

**Dysphoria**
**Vector:** Contact
**Speed:** see description
**Penetration:** 0
**Power:** 6
**Effect:** Depression, Mania, Moods

Victims experiencing dysphoria develop unpleasant moods, such as sadness, anxiety, irritability, or restlessness. Over time, these can turn into unbridled manic or hypomanic episodes or debilitating depression. Although the victim will display symptoms of unbalanced behavior and mood swings beforehand, they can worsen under appropriately emotional circumstances. Gamemasters may require the dysphoria victim to make a Willpower (1) Test. If the test fails, the character will experience depressive or manic episodes. The actual effects are left to the gamemaster's discretion.

## DISSONANT ECHOES

Submersed dissonant technomancers are able to learn both normal echoes and a few dissonant echoes of their own.

### Contaminate

A dissonant technomancer uses Contaminate to intensify the grade of Dissonance within a certain region in the Matrix, thus

corrupting it into a temporary dissonance pool—the dissonant version of resonance wells (p. 172). Dissonants particularly love to corrupt resonance wells in this manner.

To contaminate a node, the dissonant technomancer must enter it and make a Resonance + Software + submersion grade (1 Initiative Pass) Extended Test. Each hit increases the rating of the temporary dissonance pool by 1, up to a maximum rating equal to the dissonant technomancer's Resonance.

If the node was previously a resonance well, the Resonance must first be diminished before the node can be tainted. Use the same test as above, but apply a dice pool modifier equal to the resonance well's rating. Each hit diminishes the well's rating, down to zero. Additional hits past that point increase the rating of the dissonance pool, as above.

Contaminated nodes will restore themselves after (submersion grade) hours, though it is possible that dissonants may have found ways to permanently turn nodes into dissonant wastelands. This decision is left to the gamemaster.

### Malfunction

Malfunction allows a dissonant technomancer to pervert a sprite into a dissonant version of itself. To cause a sprite to malfunction, the dissonant must first reduce the sprite's tasks to 0 with Decompiling (see p. 241, *SR4A*). The technomancer adds his submersion grade to the Decompiling Test. Once all tasks are eliminated, but before the sprite fragments into Resonance code, the dissonant technomancer makes a Compiling Test (p. 241, *SR4A*) to bring the sprite under his control, adding his submersion grade to his dice pool. If the sprite is successfully recompiled under the technomancer's control, it immediately recodes into the entropic sprite version of itself (see *Entropic Sprites*, p. 179). Entropic sprites created this way may also be registered into service.

### Pryon

Nicknamed for *prions*, protein-based infectants that cause a number of diseases (such as "Mad Cow" disease), these programmable infectious subroutines can cause code-induced diseases (CIDs) that affect the neuroelectrics of the brain or other neural tissue, often with a fatal outcome. Only submerged dissonant technomancers can create CIDs. In contrast to digital viruses, these neuropathological viruses can be spread via physical contact with the submersed dissonant through his bioelectrical aura. So far, two dissonant related diseases, known as *The Black Shakes* and *Dysphoria,* have been identified (see sidebar).

### Siphon

The Siphon power enables a submerged dissonant to directly attack a target's simsense connection. In order to use Siphon, the dissonant makes a regular Matrix Attack Test using Cybercombat + Attack. The defending icon rolls Response + System instead of the normal defense roll. If the dissonant technomancer achieves 3 or more net hits, the icon is immediately dumped, suffering Dumpshock (p. 237, *SR4A*). If the dissonant scores more net hits than the target, but less than 3, the defender is instead disoriented and confused, suffering a –2 dice pool modifier for all tests for the next (submersion grade) initiative passes.

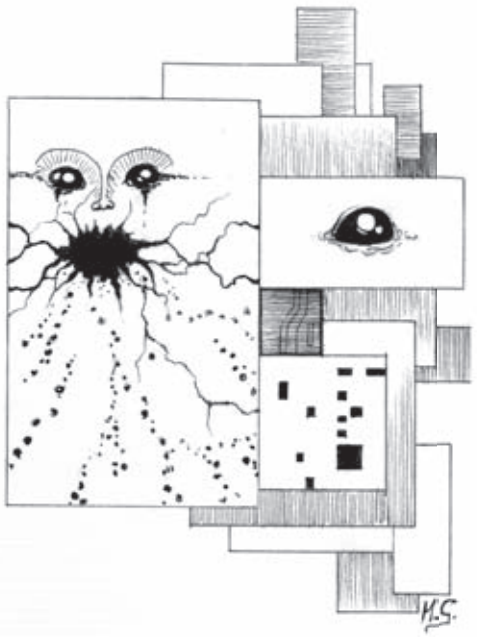
Siphon only affects personas using VR; it has no effect on AR users, agents, sprites, AIs, or e-ghosts.

## ENTROPIC SPRITES

Entropic sprites are dissonant sprites that dissonant technomancers create by twisting the code of normal sprites using the Malfunction echo (p. 179). Other technomancers can decompile these sprites, but cannot re-compile them before they fragment to bring them under their control.

The compiling and registering of entropic sprites are handled as described in the *SR4A* core rules. Although they have not yet been encountered, free and wild entropic sprites are speculated to exist. In addition to possessing unique powers of their own (left to the gamemaster's discretion), free entropic sprites can engage in dissonant versions of resonance bonds with dissonant technomancers per normal rules (p. 160).

The following five entropic sprites are those that have been encountered so far in the Matrix, though it is speculated that a myriad of other types exist. In this spirit, gamemasters are encouraged to create new entropic sprites as they deem fit.



### Blight Sprite

Blight sprites are Code or Data sprites that have been turned inside out by dissonant code. As a result, they are drawn to programmed code, corrupting and feeding on it.

| Pilot | Response | Firewall | Matrix | INIT | IP | EDGE | RES |
|---|---|---|---|---|---|---|---|
| R | R | R + 2 | R x 2 | 3 | R | R | |

**Skills:** Computer, Cybercombat, Data Search, Hacking, Software

**Complex Forms:** Attack (Shredder), Corrupt, Edit, Exploit

**Powers:** Datavore, Resonance Drain

**Optional CFs:** Analyze, Armor, Browse, Stealth

### Chaos Sprites

Chaos sprites are malfunctioning versions of Crack or Fault sprites that hack nodes to spread chaos and destruction within. Illogical malfunctions, dropped connections, and network failures are the calling cards of Chaos entropic sprites.

| Pilot | Response | Firewall | Matrix INIT | IP | EDGE | RES |
|---|---|---|---|---|---|---|
| R | R + 2 | R | R x 2 | 3 | R | R |

**Skills:** Cybercombat, Electronic Warfare, Hacking
**Complex Forms:** Corrupt, Exploit, Nuke, Node Mine, Sniffer, Spoof
**Powers:** Distortion, Siphon
**Optional CFs:** Armor, Attack, Black Hammer, Decrypt, Encrypt


### Contagion Sprite

Contagion sprites are malfunctioning versions of Courier sprites. Consisting of virulent dissonant code, they infect programs, agents, or both, creating virtual pestilence.

| Pilot | Response | Firewall | Matrix INIT | IP | EDGE | RES |
|---|---|---|---|---|---|---|
| R | R – 1 | R + 1 | R x 3 | 3 | R | R |

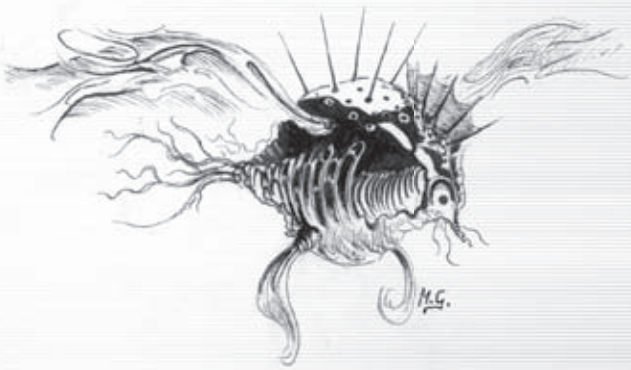
**Skills:** Computer, Cybercombat, Data Search, Hacking, Software
**Complex Forms:** Attack (Rust), Browse, Edit, Exploit, Nuke
**Powers:** Virulence
**Optional CFs:** Corrupt, Decrypt, Encrypt, Shield

### Meltdown Sprite

Meltdown sprites are corrupted versions of Machine sprites. They are adept at disabling or destroying electronic devices.

| Pilot | Response | Firewall | Matrix INIT | IP | EDGE | RES |
|---|---|---|---|---|---|---|
| R | R | R + 1 | R x 2 | 3 | R | R |

**Skills:** Computer, Cybercombat, Electronic Warfare, Hardware
**Complex Forms:** Command, Data Bomb (Biofeedback Stun or Lethal)
**Powers:** Gremlins, Surge
**Optional CFs:** Attack, Databomb (Pavlov), Decrypt, any autosoft



### Spike Sprite

Spike sprites are Fault or Tank sprites that have been infected with dissonant and BTL code. Their ability to cascade and perform Black IC attacks make them fierce opponents in Matrix combat.

| Pilot | Response | Firewall | Matrix INIT | IP | EDGE | RES |
|---|---|---|---|---|---|---|
| R | R + 1 | R + 1 | R x 2 | 3 | R | R |

**Skills:** Cybercombat, Hacking
**Complex Forms:** Attack, Attack (Psychotropic), Black Hammer, Blackout, Cascading (Rating ÷ 2, max. 3)
**Powers:** Peak, Resonance Drain, Sparky
**Optional CFs:** Armor, Exploit, Shield, Stealth

## ENTROPIC SPRITE POWERS

Entropic sprites boast some new powers appropriate to their dissonant and malicious nature.

### Datavore

Similar to the Codivore ability of AIs (see p. 168), this power is even more potent. If the sprite makes a successful attack in cybercombat, it transforms the target's damaged code into pure Dissonance, which it then sucks in to boost its own power. For every 3 points of damage inflicted on an icon, the sprite temporarily boosts its rating by 1, to a maximum bonus equal to half its starting rating (round down). This boost lasts for (Resonance) Combat Turns.

### Distortion

An entropic sprite with the Distortion power can use a Complex Action to distort all processes running on a node. This power causes a wave of Dissonance to flood through the node, causing mild feedback to all Matrix users, laced with vertigo and impaired perception. It also causes icons, images, and system iconography to fade out, waver, pixellate and de-rezz. As a result, dice pools for all Matrix Tests are reduced by the entropic sprite's rating as long as the entropic sprite sustains the power. Its effect can be sustained by spending a Simple Action each Initiative Pass past after the first to sustain it. However, during each IP, the user can roll System + Response to counter the effect, reducing the penalty by 1 for each hit.

To resonant technomancers and sprites, the distortion wave has an even stronger effect as the flow of Resonance is temporarily interrupted. If the entropic sprite beats the target in an Opposed Test pitting its Rating x 2 against their Resonance + Firewall, the target's Resonance is temporarily reduced by 1 for each Combat Turn the power is sustained. If a target's Resonance reaches zero, she is dumped out of the system, suffering physical Dumpshock with a DV that is increased by the power of the entropic sprite. This can be resisted as usual (p. 237, *SR4A*). Resonance lost in this manner restores itself at the rate of 1 point per 10 minutes.

Note that only one use of Distortion may be applied in a node at a time.

### Peak

The Peak power is used in conjunction with a normal Matrix attack. When an entropic sprite successfully hits an opponent with a regular Cybercombat + Attack Test, it can choose to zap the target with a peaked simsense signal rather than inflicting damage. This blast of simsense affects the target as if he had slotted a tripchip BTL (p. 259, *SR4A*), inflicting a negative dice pool modifier on all of the target's actions equal to the sprite's net hits for (Resonance) Combat Turns. Since the attack consists of a highly addictive dissonant BTL spike, the gamemaster may choose to have the target make a Mental Addiction Test (p. 256, *SR4A*) to check if he becomes addicted.

Spike only works on hot sim VR users, and does not have any effect against agents, AIs, sprites, or e-ghosts.

### Resonance Drain

This power is used to bleed Resonance from a victim technomancer or sprite. To drain a point of Resonance, the entropic sprite must succeed in a normal Cybercombat + Attack Test to establish a dissonant transfer connection. The entropic sprite can then drain one point of Resonance with a Simple Action each Initiative Pass. If the technomancer's Resonance reaches zero, she is dissonantly dumped out of the system, suffering physical Dumpshock with a DV increased by the power of the entropic sprite. This can be resisted as usual (p. 237, *SR4A*). Resonance lost in this manner restores itself at the rate of 1 point per 10 minutes.

### Siphon

Similar to the echo described on p. 179.

### Sparky

Same as the echo described on p. 174.

### Surge

This dissonant power targets the underlying electronics of a node, creating a range of unusual effects such as power surges and electronics malfunctions. The entropic sprite must have access to but must not be inside the device, but in a node to which the device is linked. Make an Opposed Test between the sprite's rating x 2 and the device's System + Firewall (or just Device rating x 2). Each net hit the sprite scores inflicts 1 box of damage to the device. Note that this power will have different effects depending on the nature of the device. Where a commlink might get fried or even burst into flame, a vehicle would simply suffer lose its onboard computer.

### Virulence

Virulence enables the entropic sprite to mutate a program with dissonant code so that it spawns a virus. To use Virulence, the entropic sprite makes an Opposed Test pitting the sprite's rating x 2 against the program's rating + Firewall. If the entropic sprite wins, the target program is infected with a virus (see *Viruses*, p. 120) chosen by the gamemaster.

# . . . SIMSENSE AND SKILLWARE . . .

A dog was licking Juan's face.

He smelled its breath as he woke up, reaching out and pushing its muzzle away. His head felt thick and groggy. Too much drinking, he thought. Knew it was a bad idea to hit the bars with that crazy troll girl.

The thought suddenly confused him. Hit the bars? What the hell am I thinking? I didn't hit the bars? I stayed in, studied the maps, went over plans, cleaned my gu—

His eyes popped open with a start, wide awake. He looked around in confusion. The dog skittered back and away, suddenly wary. I'm in an alley. Why the hell am I in a—

His eyes rested on the gun in his hand. His gun.

The memories suddenly came back to him, driving him to his feet. The crowds. The speaker, surrounded by bodyguards. The smarmy elf politico he had held a grudge against for months. The one he had plotted to kill. The media drones. Him, pulling his gun, shooting that liberal salad muncher right in the fuckin' face. Running from the screams, the shouts of security as they chased him °

His heart was racing. This was the alley, the alley he ran into, ducking away from the spirits and drones and armed men. Where are my pursuers?

He could hear the crowd, cheering and clapping. It wasn't the sound of a scared mob, the aftermath of an assassination. It was the sound of a lively political rally. It confused him. He cautiously moved toward the alley's mouth, carefully holding the gun out of sight.

There was the elf, still alive, leaving the stage. What the hell? I ° I just killed him! But there he was, smiling and waving, moving through the crowd, clasping hands, kissing cheeks, thanking his supporters.

Then a shot ran out. Screams filled the air. The crowd scattered like roaches. It was complete pandemonium.

Juan could only stare as someone broke from the crowd, running fast, headed straight towards the alley. That's me! He thought. He was too stunned, too flabbergasted to act. The man looking just like him gave Juan a grin as he sped past, down the alley, and out of sight.

The sickening feeling hit Juan's stomach a moment too late. I'm being set up. My memories ° that motherfucker just framed me! He started to run, to follow the man, knowing he was already too late.

"Freeze!" He knew better than to turn, gun in hand, to face the security men as they entered the alley. He knew that his only hope was to catch the man ahead of him.

The shots rang out, and he never did.

# SIMSENSE: EXPERIENCE EVERYTHING

The span of human history is dotted by transformational technologies, discoveries that have shifted the way we live in dramatic ways: gunpowder, the light bulb, the assembly line, the airplane, the splitting of the atom, and the Internet, to name a few. In 2018, Dr. Hosato Hikita unveiled another of these transformational technologies in a cramped conference room at ESP Systems in Chicago. The technology was Artificial Sensory Induction System Technology, or ASIST. With ASIST, Dr. Hikita was able to record a subject's full sensory experiences and transmit that recording to another subject's brain, invoking a copy of the senses in the second subject. The result is the ability to experience something fully without actually having experienced it first-hand. This new form of media is dubbed "simsense."

ASIST and the simsense it created have reshaped the Sixth World. Simsense has revolutionized entertainment media and skillsofts have changed the way people learn and work. The Matrix was built on an ASIST framework and the augmented reality of today's Matrix would not be possible without advances in the same basic technology that Dr. Hikita showed off in 2018.

## ANATOMY OF AN ASIST SIGNAL

When you listen to a piece of recorded music, you are actually listening to a collection of tracks made up of numerous frequencies of sound. Each of the instruments and the vocalist are usually their own track and within each track the sound includes different frequencies which can be isolated. Similarly, an ASIST signal is a collection of tracks, each one representing a different sense or emotion. The sensory tracks are divided into *exteroceptive* and *interoceptive* tracks. Exteroceptive tracks include the traditional senses of sight, smell, hearing, touch, and taste that process the outside world. Interoceptive tracks include senses originating within the body, such as balance, a sense of motion, pain, hunger and thirst, and a general sense of the location of one's own body parts. ASIST engineers define experiences by how they register on the various tracks. For instance, the experience of looking at a cloud will register almost exclusively on the exteroceptive sight track. The experience of falling registers almost exclusively on the interoceptive balance track. The experience of smelling freshly baked blueberry muffins registers on the exteroceptive smell and taste tracks, but could also register on the interoceptive hunger track.

Emotive tracks are divided by the neurobiological systems they evoke, which in turn activates or suppresses an emotional response. Some of the emotive tracks typically used include the sympathetic, parasympathetic, adrenal, thalamic, hypothalamic, and limbic tracks. They will control pleasure and pain, wakefulness, blood pressure, fight-or-flight instinct, sexual arousal, short- and long-term memory, rational thinking, mood, and many other emotional responses.

Like the frequencies of a song's vocal track, each track in an ASIST recording also carries a three-dimensional signal map that corresponds to the position of an electrical signal in the brain and the strength of that signal. Over the length of a track, different areas of the brain are stimulated at different strengths, invoking the sensory and emotive responses in the subject's brain. The combination of these signals is what creates the simsense experience.

A simsense recording is classified in one of two ways, depending on the tracks it carries. *Baseline* recording includes only the sensory tracks. A user experiencing a baseline recording will get the full sensory experience, but their emotions will be their own. *Full-X* ("full experience") recordings include the sensory and emotive tracks. Users experiencing a Full-X recording will find their own emotions influenced or dominated by the emotive tracks of the recording, depending on the strength and quality of the signal.

## PRODUCING A SIM

A great simsense experience is more than just a good EC/IC modulator chip or autonomic response smoothing processor. Excellent performers, a skilled director, and a talented post-production team can separate last year's forgotten straight-to-baseline release from this year's award-winning blockbuster. The sim industry, like the film, television, and music industries before it, comes down to the indefinable "star quality" of its talent.

### The Cast

No matter how many actors are in a given sim production, usually only a handful are wired for simsense recording. These actors will almost always have implanted simrigs; trodes produce inferior recordings and are only used on low budget projects. Wired actors are known as *performers* in the business, while the other actors are *flats* (extras that provide background in a scene), *props* (actors who interact verbally or physically with the wired performers) or *targets* (actors who are involved in complex and interactive scenes with the performers, such as fight scenes or love scenes).

The number of wired performers is kept to a minimum because each performer is providing a separate point-of-view (POV) in the production. Adding multiple POVs is not only expensive, but it also makes it harder to tell a cohesive story. It is also typical that only one or two performers are wired for Full-X recording, while the others only record in baseline. Cost is one factor here, but there's also the fact that only top-notch simsense performers can provide a convincing emotive recording that can fool an audience. True simstars are often method actors to the highest degree, literally becoming their role as an effective method of producing utterly convincing emotional states.

Nearly all sim productions release with just one or two POVs, usually the protagonist and a single supporting role. Special edition releases produced later will add on other POVs, such as other supporting roles or the antagonist. There's a strong market for bonus POVs from the villain's perspective.

### Tricks of the Trade

Sim performers are kept in peak physical condition. When an audience is feeling every aspect of the performer's experience, they don't want to be experiencing lower back pain or a wheezing cough. Those undesirable experiences can be scrubbed in post-production, but if a studio wants to get the most out of its performers, it will keep them in good shape. For a Full-X performer not in their prime form, tricks such as medication and hypnotherapy are sometimes used to elicit particular emotional responses. Some desperate performers have even turned to personafixes and other BTLs to prepare for a role, but those efforts can burn out a per-

former prematurely and leave them one of the many sad, has-been husks that litter the entertainment world.

Sim productions try to avoid using doubles, because the entire point of a sim is for the audience to experience the performer, not an unknown double. But in cases where a double is necessary, a method called *stacking* is used. In stacking, a double is run through a scene and recorded in baseline only. Then the star performer plays back the double's baseline through her own sensorium and a Full-X recording is taken. The emotive tracks aren't as authentic as the real thing, because the performer is responding to recorded senses and not her own, but it does allow for scenes that might be too dangerous to risk a star performer on. Studios will often keep libraries full of *sense-patches* on hand, which are pre-recorded baseline tracks of doubles in stock experiences. These sense-patches are not particularly innovative and fresh, but they can save a production tens of thousands of nuyen.

*Pseudosim* is another trick used by the sim industry, where the simsense tracks are entirely computer-generated; a sim performer is not involved. This is common in simsense games, where player actions change the story and many possible permutations of sensory data must be accounted for. But it can also be found in simflicks where the performers need to interact with computer-generated props and targets. If Neil the Ork Barbarian needs to fight a dragon in his latest simflick and Lofwyr isn't available, a computer-generated dragon is used and pseudosim tracks are layered over the barbarian's recording to convince the audience they are fighting a real wyrm. The technology exists for fairly convincing baseline pseudosim, but Full-X pseudosim is still clumsy and unconvincing, which is why there aren't any hit simflicks from the dragon's emotional point of view.

If a studio has some serious cash behind a production, they may use magical illusions instead of pseudosim. If a skilled magician casts an illusion, the performer cannot differentiate the illusion from reality, so the ASIST recording of the fight with the dragon is as convincing as if a real dragon was co-starring. However, though physical illusion spells can be recorded on camera, they cannot be wired for even baseline ASIST recording. So if you want to add the dragon's POV, you either need to go with a pseudosim approximation or you need to hire a living, breathing dragon.

### The Wet Record

The *wet record* is what you get after you are done recording a sim production; it's the raw ASIST recordings from each performer. Pure, uncompressed ASIST recordings are massive files that require expensive storage to keep on hand and all wet records are kept under tight security. These days only pre-edit master copies of simflicks are kept in uncompressed ASIST; commercially available copies have all been transcoded into more portable compressed formats. However, there are some simsense aficionados who will do just about anything to get their hands on a wet record copy of their favorite simflicks, prizing the most authentic sim recording possible.

Because of the costs involved in recording ASIST (production costs, storage costs, and the mental cost on performers), a good director is worth their weight in gold. A skilled sim director is part psychoanalyst, able to understand what will provoke the right emotional responses in his stars and able to build the conditions to bring out the stellar performances. Being a sim director can take its toll, however. Most sim directors plug straight into the ASIST feed of their performers during recording to get a sense if the scene needs another take and constant exposure to pure ASIST has led more than one hit director down the road to ruin.

### THE HISTORY OF SIMSENSE

**2018:** Dr. Hosato Hikita of ESP Systems successfully demonstrates the first ASIST recording to the public.
**2024:** The first commercial simsense gear is sold, but only to research labs and the ultra-wealthy.
**2029:** Sony, Fuchi, and RCA-Unisys develop the first ASIST cyberterminals, sensory deprivation tanks surrounded by a room full of computer hardware.
**2031:** Second generation cyberterminals integrate the sensory deprivation tank and computer hardware into a desk-sized cocoon.
**2036:** The Fuchi CDT-1000 third generation cyberterminal eliminates the sensory deprivation tank and is reduced to a desktop box.
**2037:** Fuchi unveils RealSense, adding an emotive track to simsense recordings.
**2043:** Skillsoft technology is developed, allowing ASIST to transmit skills to a user who does not know them.
**2046:** *Free Fall*, starring Holly Brighton, breaks sim records and pushes simsense technology into the mass market.
**2050:** The first generation of cyberdecks—keyboard-sized cyberterminals—are released.
**2052:** 2XS, a more addictive form of better-than-life simsense, becomes a deadly craze.
**2064:** Transys-Neuronet and Erika Corporation build the first broadcast wireless ASIST network in Stockholm.
**2066:** First generation commlinks—palm-sized cyberterminals—are commercially released.

### Simsynths

To all but the most purist simfreak, a wet record is unsatisfying, full of underwhelming emotional moments, background noise like the normal aches and pains of existence, and unpleasant sensory and emotive spikes. That's why every wet record goes into post-production before release and is polished down into a final product. The key component of simsense post-production is the ASIST signal processor, or simsynth.

A simsense technician will feed each point-of-view wet record into the simsynth to clean up the signal. A good simsynth will allow him to boost weak EC/IC (exteroceptive/interoceptive) sensory tracks and splice in sense-patches where there are sensory gaps. It will also smooth out the high- and low-end signals which are unique to each and every performer but can be jarring for some users. High-end studio simsynths will allow for simultaneous cross-processing, meaning the technician can edit more than one

POV wet record simultaneously, which can be crucial when you want to get the two POVs in the climatic fight sequence meshing up just right. When the technicians have the final *experience record* ready, they use the simsynths output samplers to transcode the record into a compressed format that can be put down onto media or broadcast wirelessly.

Simsynths range in quality and cost, from small prosumer models that can modulate only a few EC/IC baseline tracks and process only a single POV to high-end studio simsynths that have forty-eight racked EC/IC modulators, polyPOV cross-processors, full emotive mapping software, and samplers that can output in just about any compression format known.

## EXPERIENCING A SIM

A studio can create a masterpiece sim, but unless it can be experienced, it won't mean a thing. Fortunately, experiencing sims is simple these days, since many commlinks include a sim module that can process ASIST. Even though experiencing a sim is easy now, there are still a few considerations to keep in mind.

### Output Formats

Nobody markets wet records, even though there are a handful of freaks out there that would buy them. The simflicks that you and I experience have gone through post-production and have been sampled into a compressed format that is easier to distribute. The compressed ASIST is either broadcast over the Matrix or burned down to a piece of storage media and then our sim modules or sim decks uncompress the ASIST during playback. The three most standard forms of compression are listed below, though many others exist.

**Direct Experience Format (DIR-X)** is a lossless form of ASIST compression, meaning that when uncompressed the simsense signal is identical to the pre-sampled signal; no signal quality is lost whatsoever. Aside from the wet record, this is the closest you can possibly get to actually being there and actually *being* the performer. However, DIR-X files are massive and are impractical for broadcasting over the wireless Matrix. Most wireless users don't want to wait for hours for their sim to transfer and many nodes will block file transfers of this size to prevent them from bogging down their bandwidth. For this reason, DIR-X is usually only used for special theatrical releases or for special edition pay-per-view transfers. Despite being impractical, there is a small market out there among simphiles for DIR-X recordings.

**ASIST Control Transport (ACT)** is a far more common form of simsense compression recognized by all commercial simdecks and sim modules. ACT files are about one percent of the size of the same recording in DIR-X, but that file size comes at a loss of signal quality. ACT works by sampling only specific signal maps on each track instead of the whole thing and then adds a command set to the file. This command set instructs the sim module or simdeck to approximate the missing pieces using the user's own senses and emotions and a standard library of sensory/emotive tweaks. So in a scene where you are supposed to feel Nicky Saitoh's raging anger, you are instead feeling your own raging anger tinged with a bit of what it is like to be an angry Nicky Saitoh. Most users won't know the difference, however. How well a sim module can interpret the command set depends on the quality of the sim module, so your experience will get better on better playback machines. The manageable size of ACT files makes it the primary compression method used for simflicks, whether they are distributed on storage media or broadcast over the wireless Matrix.

**Scalable ASIST Stream Format (SAS)** is the most popular format used for all those augmented reality overlays and is understood by all sim modules. The important thing about SAS is that it allows for better compression by prioritizing tracks and by relying heavily on a command set to approximate the signal using the user's own senses and emotions. Since emotive tracks are rarely used in augmented reality and even then only on a rudimentary level, the emotive tracks are sampled infrequently. Similarly, since augmented reality doesn't need the user to reproduce a specific performer's ASIST, it can put most of the work on the sim module and sample less of the ASIST. If Stuffer Shack wants their AR ad to make a user feel hungry, they don't care if you feel the same hungry that Joe the Out-of-Work Sim Performer felt, so they let the sim module approximate your own feelings of hunger. Simflicks are almost never distributed in SAS format because it removes the major draw of simflicks, the ability to experience something as if you are someone else.

### Playback Gear

On the most basic level, all that is necessary to play back an ASIST file is a sim module (p. 226, *SR4A*). Since a sim module is a common option for commlinks, nearly everyone can play back ASIST on their commlink. However, commlinks are the Swiss Army knives of the wireless Matrix and while they can convert ASIST into acceptable play back experiences, the ASIST processors in their sim modules are geared more towards interpreting virtual reality pseudosim and augmented reality SAS format ASIST. If you want the best quality when you play back your ACT format simflick release, you really want a *simdeck*.

Simdecks are set-top boxes with high-end ASIST processors designed for simflick playback and pseudosim game rendering. Even a neophyte sim user can tell the difference between a simflick experienced on a commlink and one experienced on a simdeck. The experience is more real. They are also far superior for processing the computer-generated pseudosim used in many sim-games, making them the gaming consoles of choice. Even though a commlink can handle multiple simultaneous POVs through multiple subscriptions, the dedicated simulPOV ports on a simdeck make for a far more enriching experience.

A sim module or simdeck translates the computer data into precise locations and amounts of electrical and ultrasound signal to be applied to the brain (and vice versa), but you still need a piece to do the actual application, either trodes or a direct neural interface. Any simfreak will tell you that DNI is the way to go, because the electrodes and ultrasound emitters are inside the brain and the signals aren't weakened by the skull the way trode signals are. The same simfreak will also tell you that if you don't have DNI, you're better off with standard trodes than nanopaste trodes. Sure, nanopaste trodes will get the job done, but the signal application is less precise (depending on how well you apply the nanopaste) and the signals tend to be weaker. The rule of thumb is: the less resistance between the emitter and the brain and the more precise the signal can be targeted at specific regions of the brain, the more real the simsense experience.

Speaking of trodes, it used to be that a trode net was an ugly hairnet-like collection of electrodes and ultrasound emitters that users would try to conceal under headbands, hats, or wigs. While those trode nets do still exist, Renraku's DreamBand and Horizon's E-piphany trodes have made trode-wearing stylish. These trodes use the latest technology to conceal all the electrodes and ultrasound emitters in a stylish band that hooks over the ears and wraps around the back of the head. Still not as pure a signal resolution as DNI, but at least now you don't have to get brain surgery or look like a McHugh's cook to enjoy your sims.

## LEGAL CONSTRAINTS: REALER THAN REAL

ASIST is a revolutionary technology, and like most other revolutionary technologies it hit the market before the risks could be entirely considered. By the time the risk had been considered, ASIST was such a hit that users didn't really care about the possible dangers. Worse yet, corporate deregulation had put much of the research into the risk of ASIST into the hands of the same corporations that sell it. It should be no surprise that this research backs the attitude that simsense is entirely safe if used as directed.

## HOOKED ON SIMSENSE

The dangers of better-than-life addiction have long been known, but there are those who claim that even "safe" levels of simsense are addictive and dangerous. Since the early 2040s there have calls for the regulation of simsense, claiming that frequent users of simsense become withdrawn from the real world. A handful of nations prohibit the sale of simsense to minors, but these are mostly nations where simsense technology is uncommon to begin with and not the media-saturated first world nations. There are also some companies that sell software that allows parents to restrict the amount of simsense their children can watch, but adults have no such restrictions.

There are endless corporate-backed research studies that "prove" that the simsense that is legally and commercially available is completely safe. But observation does show that many frequent simsense users do become withdrawn from reality. Some critics argue that even safe simsense invokes the pleasure centers of the brain in the same ways that drugs and alcohol do and therefore can become addictive. Supporters of the technology do not entirely refute this claim, but frequently remind people that chocolate and sex also affect the pleasure center of the brain and yet neither one of those is regulated.

Regardless of where the reality of the addiction argument falls, one thing is for certain. Simsense allows one to enjoy a crafted reality that is as real to them as the real world is, but usually doesn't include the shit that the real world loves to heap on us. That's a convincing enough reason for a frequent simsense user to become withdrawn from the real world.

## SUBLIMINALS

Once upon a time, there was a debate about subliminal advertising, where frames depicting something would be flashed quickly in a video stream. The idea was that it happened so fast that the viewer would not consciously notice it, but that the brain would process the frames anyway. Scheming advertisers thought that maybe the brain could be fooled without the viewer's knowledge and that the brain would remember the frame and shape the viewer's future thoughts. Research concluded, however, that the influence of these subliminal frames was minimal, that they happened so quickly and the brain processed them to such a limited extent that they were quickly forgotten and had no lasting persuasive effect.

Simsense offers a new approach to subliminals, though. With simsense, sensory tracks can be matched up with emotive tracks that normally have no realistic association to the sensory information being experienced. Associative conditioning like this has been used for ages; the old adage "sex sells" describes how advertisers used sexual imagery to condition you to associate their product with sexual attraction and arousal. But those advertisers depended on *you* to make the association. Simsense rams the association straight into your brain without any conscious thought necessary.

Let's say Aztechnology wants to sell some NukIt burgers. They start running some augmented reality advertising that when experienced with simsense allows you to smell and taste a delicious NukIt burger, even feel the warmth radiating from it. But Aztechnology wants to make you desire a NukIt burger more than any other burger, so they layer emotive tracks that make you feel

satisfied, happy, or even sexually aroused near the advertisement. If you are subjected to this advertisement enough, your brain may start to associate NukIt burgers with pleasure and that may encourage you to buy them, even though the real NukIt burger experience is hardly pleasurable.

This kind of subliminal simsense has been around since ASIST first appeared, but the ubiquitous nature of augmented reality has made it a hot topic again. Many nations have laws against subliminal simsense advertising and even the Corporate Court has regulated it to prevent it from getting out of hand. But most of these laws are difficult to enforce, requiring a plaintiff to prove that the object being advertised does not cause the emotional effects he alleges are produced by the advertisement. Proving that a NukIt burger doesn't make anyone happy is a tough case and even if the plaintiff wins, the corporation is usually just fined. Those fines hardly ever deter a corporation from the sales that subliminal simsense advertising can bring in.

## PEAK CONTROLLERS

Peak controllers are what separate "cold" sim from "hot" sim and what separate simflicks from better-than-life chips. They are legally-required modulators on sim modules that enforce safety standards. Peak controllers limit ASIST signal in a number of ways. First, they prevent an ASIST file from calling on trodes or DNI to deliver damaging levels of electrical or ultrasound signal to the brain. Second, they limit how an ASIST file can call on autonomic regions of the brain, ensuring that simsense can't cause you a great deal of pain or increase your heart rate to dangerous levels. Third, they limit how frequently and how intensely an ASIST file can reference the pleasure centers of your brain, in order to (supposedly) prevent simsense use from being addictive. There are more limits than those three, but those are the big ones.

Mandated peak controllers are part of the Business Recognition Accords, so corporations must put them in their product according to national laws in order to sell the product in that nation or import it to that nation. However, the exact levels of where peak controllers cut out vary from nation to nation, which has created a thriving black market for more intense simflicks. In addition, many hacks exist for disabling peak controllers in simdecks and sim modules, letting simfreaks and hackers juice up their signal. Modifying a sim module or simdeck to remove the peak controllers is the same as modifying a sim module for hot sim and requires a Hardware + Logic (10, 1 hour) Extended Test.

### California Hots and Kong Chips

There are two places of note which have a combination of a thriving simsense industry and weaker-than-normal peak controller mandates. Los Angeles and the Hong Kong Free Enterprise Zone both legally allow for simsense recordings to have content outside the peak controller limits of other nations. While not quite Better-Than-Life chips, California Hots and Kong Chips, as they are respectively known, are both more addictive than typical simflicks. Los Angeles requires that these more powerful sim recordings carry a Surgeon General's warning, but the studios have turned that warning into an advertisement. "This Surgeon General has found this plot to be too wild for the weak of heart and advises that it may be too much to handle!" In Hong Kong, not even that back-handed effort is necessary.

Of course, these enhanced simflicks never stay in the nations where they are legal and criminal syndicates smuggle them onto the black market in other nations, selling them for inflated prices as rare commodities.

### Bootleg and "Enhanced" Sims

Commercially available simflicks are often run through a peak controller twice, once during post-production before the final experience record is created and once during playback in the sim module or simdeck. Original, unedited wet records have not passed through the post-production peak controllers and so if played on a modified hot sim module or simdeck, they will retain the full experience. These bootleg sims are worth a lot of money to true fans and shadowrunners are often hired to steal wet records from the studios (studio security is usually too tight for a simsense technician to just smuggle them out).

Then there are those who make after-market alterations to legal simflicks, decrypting them and hacking them in order to add stronger sense-patches to scenes. These "enhanced" simflicks are not as valuable as the bootlegs (because the authenticity isn't there) but there are those who purchase them just for the added rush.

### Snuff Sims

It is a sad fact of the Sixth World that snuff sims exist. Snuff sims record the final moments of the performer as they die, most often the result of murder. Because the recording captures the pain, fear, and panic of the victim, they can be dangerous to the user and are often run through a peak controller to prevent risk. However, there have always been rumors of snuff sims without peak controller limits, sims so real and so deadly that they can kill those who experience them. Whether or not these rumors are true, the risk is certainly there. If a user experiences a snuff sim without peak controller limits (either on the sim or in their sim module), they must make a Body + Willpower (3) Test or suffer a potentially fatal heart attack. Even those who succeed in the test are often left with Negative Qualities from the trauma of the experience.

Snuff sims are highly illegal, even in nations with lax simsense regulation laws. Simple possession of a snuff sim can carry harsh prison sentences. Possession with the intent to distribute or distributing snuff sims can carry long prison sentences and even death sentences in some nations.

## REALITY AMPLIFIERS

Reality amplifiers (or "amps") are an offshoot of Better-Than-Life chips, originally researched as a replacement for military combat drugs. While Better-Than-Life chips tend to overwrite a user's natural sensory or emotive information with more powerful ASIST signals, reality amplifiers boost naturally occurring sensory or emotive information in the brain. The benefit of reality amplifiers over combat drugs is their instant-on, instant-off nature. Like BTLs, they can be accessed as programs on a hot sim-modified commlink or sim deck, or as a direct input chip via datajack. The downside of reality amplifiers is that like Better-Than-Life chips, the amplified signals are addictive and prolonged use can cause psychological problems. Unlike direct input BTL chips, amps

by default can be used repeatedly and are typically much more expensive. Some criminal syndicates have started selling cheaper, one-shot amps.

### Breakdown

Unlike the other amplifiers, Breakdown amplifiers were not designed to be used by soldiers. Instead, Breakdown amplifiers were intended to be applied to prisoners against their will. A Breakdown amplifier boosts pain signals in the brain and enhances signals from the amygdala that control reward- and fear-related motivational decisions. The effect is that it makes the prisoner more pliable to intimidation and interrogation. If a Breakdown amp is active, the user suffers a –2 dice pool penalty on Willpower + Intimidation Tests made to resist intimidation and interrogation (p. 130, *SR4A*).

### Focus

Focus amplifiers are the opposite of Red Alert amps. Focus activates the parasympathetic nervous system, which causes the fight-or-flight response to end and returns the body to a calm state. A Focus amp can be activated to eliminate dice penalties due to distracting or stressful situations. With a Focus amp running, a hacker can calmly write code while taking heavy fire. A Focus amp cannot be running at the same time as a Red Alert amp, even if the user has more than one datajack.

### Oracle

An Oracle amplifier boosts exteroceptive sensory data before it reaches the brain. The sensory information taken in is the same, but it is processed by the brain at a much higher clarity. The effect is that the user's senses of touch, taste, sight, smell, and hearing are improved while the amp is active. An Oracle amp adds +2 dice to all physical Perception Tests made while it is active. Oracle amps come with safety breakers, so in the case of overwhelming sensory input (very bright lights, loud noises, etc.) the amplifier will shut off. Oracle amps do not add dice to Astral Perception Tests or Matrix Perception Tests.

### Red Alert

Normally an outside stimulus is required to trigger the fight-or-flight response in the sympathetic nervous system. A Red Alert amplifier, however, activates the sympathetic nervous system as soon as it is slotted, putting the user at a constant alert state. Red Alert amps add +1 dice to all physical Initiative Tests, including the Initiative Test used to determine Surprise. Red Alert does not benefit Astral or Matrix Initiative Tests. While a Red Alert amp is active, it is difficult to concentrate on sustained tasks. Any Extended Tests have their thresholds increased by three as long as the amp stays active.

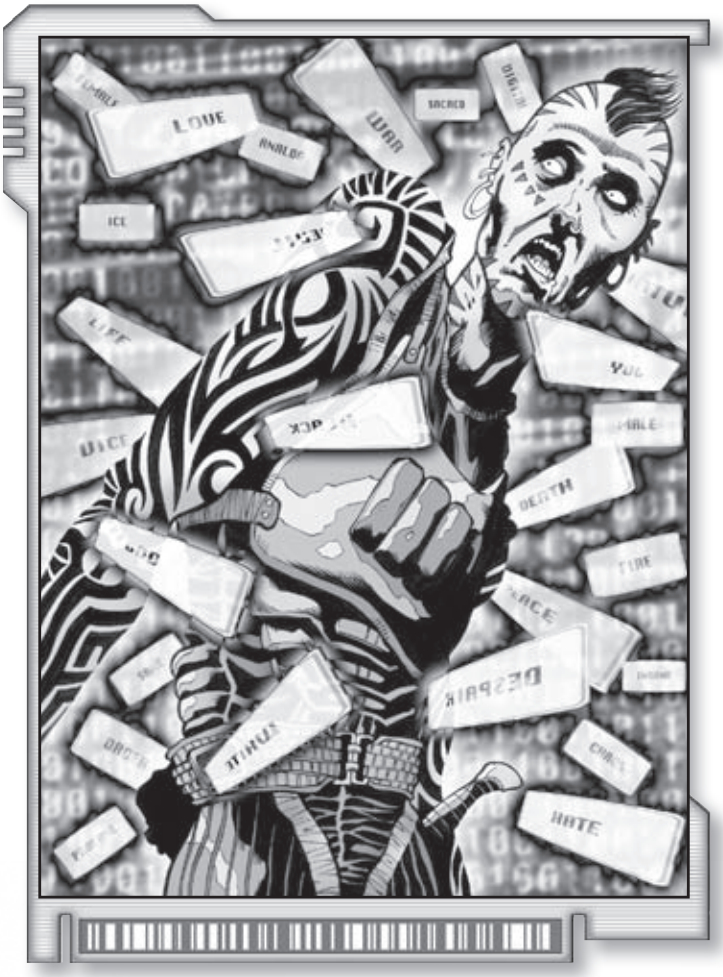
## BRAINWASHING: PROGRAMMABLE ASIST BIOFEEDBACK

Take one solid look at a beetlehead and you can see that simsense can be bad for the brain. ASIST manipulates and fools the brain, removing the barrier between reality and fantasy. To some, ASIST had too much potential to be limited to entertainment or be held back by ethics and regulations. For decades, powerful militaries, shadowy intelligence agencies, and anonymous corporate laboratories conducted ASIST experiments on prisoners, psychiatric patients, and other undesirables. It was discovered that carefully controlled and specific application of ASIST would leave an imprint on the brain even long after the signal was shut off, forming false memories and experiences. Programmable ASIST Biofeedback—as the technique is known—is far more than traditional brainwashing; it is the clinically precise reprogramming of a metahuman being.

### SETTING THE STAGE

The key piece of any ASIST programming session is the **Programmable ASIST Biofeedback (PAB)** unit. The dark cousin of the simsynth, a PAB unit takes a lossless DIR-X signal and dissects it, looping certain sequences, removing peak controls at key points, and amplifying channels that build memory, such as the sense of

| Software/Chip | Availability | Cost |
|---|---|---|
| Reality Amplifier | 14R | 500¥ |




smell. PAB units vary in size and quality. There are low-rating, briefcase-sized units for the busy brainwasher on-the-go, while the high-rating, non-portable units utilize racks of equipment and are often built into clinic rooms with a controlled environment. PAB units are highly restricted and to legally acquire and use one requires a license typically reserved only for specialized therapists.

The PAB unit does the heavy lifting in any brainwashing session, but the modified signal still needs to be fed into the subject's brain. Because peak controls are disabled on certain pieces of the signal, the subject is often patched into a hotsim-modified simdeck during the brainwashing procedure. Then a direct neural interface or a set of trodes is used to feed the signal onto the subject's brain. Tests have shown that the higher signal clarity of the playback gear, the easier the programming is, presumably because the ASIST sequences are more convincing.

It is not necessary to drug the subject during a brainwashing session, but it is common for sedatives to be used. The sedatives serve a dual purpose: they help keep an unwilling subject controlled and they often make the subject's brain more susceptible to the brainwashing. In the most extreme cases, gamma-scopolamine (p. 255, *SR4A*) is used to assist in programming unwilling subjects.

## EVENT REPROGRAMMING

Event reprogramming is the most common use of programmable ASIST biofeedback. It consists of inserting false memories and removing real ones. Though the experiences are fabricated, the memories of them created by the ASIST programming are real. The subject will truly believe they happened and even interrogation will not reveal the truth. Lie detectors, truth serums, even torture will indicate that the subject is being honest about his remembered experiences. Similarly, memories removed by event reprogramming cannot be recalled unless the subject undergoes deprogramming (see below). Even qualities such as Photographic Memory (p. 92, *SR4A*) or adept abilities like Eidetic Sense Memory or Three-Dimensional Memory (p. 176, 180, *Street Magic*) will not allow for the retrieval of these removed memories.

Event reprogramming cannot change the subject's behavior, but the false memories can influence the subject to behave differently. For example, event reprogramming can't make the subject hate a particular person, but implanting memories of the subject being repeatedly abused by a particular person can give the subject sufficient reason to hate them.

To attempt an event reprogramming, the subject must first be connected to the PAB unit and then the programmer must make a Psychology + PAB Unit Rating (subject's Willpower, 1 week) Extended Test. Threshold modifiers apply to the test depending on the nature of the reprogramming, as shown in the Event Reprogramming Modifiers Table (p. 191). Event reprogramming is methodical and demanding work; the programmer must devote at least eight hours a day every day of the interval week in order to attempt a test. If an interval is missed either because of interruptions or because the required eight hours was not put in, the event reprogramming test must be restarted.

If the event reprogramming test is successful, the subject's memories have been altered as intended. In addition, any recollection of the event reprogramming session itself will be removed and the programmer can insert false memories

| PAB Units | Device Rating | Availability | Cost |
|---|---|---|---|
| Sony 800AL Field PAB Unit | 1 | 14R | 6,000¥ |
| DocWagon Cleansweep | 2 | 14R | 8,000¥ |
| MCT MemEdit III Suite | 3 | 14R | 10,000¥ |
| Interneurox G-Series Memory Master | 4 | 16R | 13,000¥ |
| Transys-Neuronet MES Grand | 5 | 18F | 16,000¥ |
| Renraku MR-X ASIST Reprogrammer | 6 | 20F | 20,000¥ |

to explain the missing time. Also, although the subject is exposed to hot-sim levels of ASIST during the programming, the process is carefully monitored so that the subject expresses no addiction to hot-sim after the programming.

If the event reprogramming test fails, the altered memories are not correctly applied and do not hold. The GM may decide the actual effects, but the result should involve patchy and confusing memories that betray themselves to be false after a few days. Failure due to a critical glitch should be far more serious, with lasting damage done to the subject such as amnesia, schizophrenia, phobias, or severe BTL addiction.

### EVENT REPROGRAMMING MODIFIERS

| Situation | Modifier |
|---|---|
| Altered memories span a period of: | |
| Less than a day | –1 Threshold |
| Less than a week | 0 |
| Less than a month | +1 Threshold |
| Less than six months | +3 Threshold |
| Less than a year | +6 Threshold |
| More than a year | +8 Threshold |
| Altered memories are insignificant to subject | –1 Threshold |
| Altered memories are very significant to subject | +2 Threshold |
| Subject is directly involved in altered memories | +2 Threshold |
| Altered memories involve a series of events | +1 to +4 Threshold (GM's discretion) |
| Altered memories conflict with basic behavior* | +1 to +4 Threshold (GM's discretion) |
| Concealed Reprogramming | Variable† |

* Apply this modifier if the subject or well-known people in the altered memories behave uncharacteristically, conflicting with the subject's own behavior or the other person's behavior in other, unaltered memories. For instance, if the normally pacifistic subject lashes out violently at someone in the reprogrammed event, the modifier would be applied. Similarly, if a friend who the subject has known for years (and retains those memories) acts as if they don't know the subject in the reprogrammed memory, apply the modifier.

† The programmer can choose to conceal evidence of the reprogramming more thoroughly than usual. The programmer chooses the number to increase the threshold by and this same number acts as a modifier against detecting the event reprogramming (see Detecting Reprogramming, p. 191).

## DETECTING REPROGRAMMING

Realizing that something is wrong with one's memories may not be particularly difficult. The opinion of a witness or recorded evidence of an event differing from the subject's recollection can be enough to tip off the subject that something is off about their memory. But actually determining that ASIST reprogramming is the reason for the discrepancy and targeting where the ASIST reprogramming was done in order to reverse it is far more difficult. Extended psychotherapy is often needed, including the use of deep regression hypnosis or PAB units to pinpoint the altered experiences. It is important to note that unless someone is specifically investigating the reprogrammed memories, it is very unlikely that it will be noticed accidentally. A reprogrammed subject could visit a therapist regularly for years and unless there is reason to look into the altered set of experiences, there would be no reason to question their programmed memories.

In order to specifically examine a subject's memories for signs of alteration, a Logic + Psychology (12, 1 day) Extended Test must be made. The threshold for this test is modified in two ways. If the original event reprogrammer modified his test using Concealed Reprogramming, then the number his threshold was increased by also increases the threshold of this test. The threshold can be lowered if the examiner uses a PAB unit of their own to monitor the subject during the psychological examination. In this case, lower the threshold by the rating of the PAB unit.

This test should be rolled in secret and if the test fails, the gamemaster should simply report that no reprogramming was detected in the examination. If the test is successful, the examiner can determine that the subject was reprogrammed using programmable ASIST biofeedback and they also know which memories were altered. Actually undoing the reprogramming requires a separate step covered in Reversing Reprogramming, below.

The Mind Probe spell may be used as an alternative way to detect ASIST reprogramming. Like the Psychology Test, this roll should be made in secret. The spellcaster must be specifically investigating a set of memories for this method to work. Three hits on the spellcasting test will determine that some ASIST reprogramming has taken place on the targeted memories. Five hits are necessary to determine the exact extent of the reprogramming so that it can be reversed.

## REVERSING REPROGRAMMING

Reversing event programming works almost identically to the process that installed the original programming. In fact, the therapist attempting to reverse the programming must make the exact same extended test that the original programmer made, rolling Psychology + PAB unit dice against a threshold equal to the threshold of the original programming (see *Event Reprogramming,* p. 190) with the same interval of one week. Reversing reprogramming is not as strict a process as the original reprogramming, however. The weekly sessions are hours long and may take multiple days, but they do not require constant

eight-hour daily work for the entire week. Also, reversing reprogramming can be interrupted and returned to later with no penalty, though the subject will not remember their true memories until the test is successfully completed.

The only additional modifier to this roll depends on the PAB unit rating the therapist is using during the reversal process. If the therapist's PAB unit is rated higher than the one used in the original reprogramming, the threshold is reduced by the difference. If the original reprogramming used a higher rated PAB unit, then the threshold is increased by the difference. Unlike event reprogramming, it is possible to reverse reprogramming without the aid of a PAB unit, but doing so means the therapist can only use their Psychology dice on the roll and the rating of the PAB unit used in the original reprogramming increases the threshold by its full rating.

If the reverse reprogramming test is successful, the subject's memories are restored to their original, unaltered state, including the memories of the actual reprogramming session. If the test fails, no harm is done, but the altered memories remain in place, even though the subject now knows they are not real. If the reverse programming test fails due to a critical glitch, the side effects can be the same as a botched reprogramming, including amnesia or schizophrenia.

### INVOKED PROGRAMMING

Invoked programming is a variation of event reprogramming, where implanted or concealed memories are inaccessible until a pre-programmed trigger event occurs. Actual memories can be blocked, leaving gaps in the subject's memory that come rushing back when the trigger event takes place. Alternately, false memories can be programmed that are not invoked until the moment the trigger event occurs, at which time they come flooding in.

The trigger event must be selected during the event reprogramming process, but it can be virtually anything. It can be a certain phrase, a particular date in time, or even a set of experiences that must happen in order to trigger the memory. The rush of memory that is invoked when the trigger event occurs is very disorienting. Any test made within one Combat Turn of hidden memories being invoked suffers a –2 dice pool modifier.

Like other event reprogramming, traditional interrogation techniques will not uncover the hidden memories if the trigger event has not occurred. Successful detection and reversal of the event reprogramming will make hidden memories available again or can remove hidden false memories. Hidden memories can be invoked with 5 hits on a Mind Probe spell, assuming the magician knows to look for them. Mind Probe can only reveal hidden memories; it cannot remove false memories that had been hidden.

Invoked programming is rarely used, but it has been implanted in reprogrammed double agents or deep cover infiltrators. It allows the asset to be inserted among his targets with no knowledge of his mission or background until he is activated by the trigger event.

### BEHAVIOR MODIFICATION

Programmable ASIST biofeedback can be used for more than implanting or erasing specific memories and experiences. In fact, the most common legal use of programmable ASIST biofeedback is in treating addiction or mental disorder. By targeting memories associated with trauma or addiction, the behavior itself can be modified. Unfortunately, even this medical miracle has been perverted by those who would use it as a weapon. Just as programmable ASIST biofeedback can be used to remove these problems, it can also be used to force them onto people by creating mental trauma or addiction.

The test for modifying a subject's behavior using PAB is similar to the test for Event Reprogramming; only the threshold is different. The person attempting the behavior modification engages in a Psychology + PAB Unit Rating (Quality BP cost, 1 week) Extended Test. The threshold is the build point cost associated with the negative quality being treated or implanted. Positive qualities cannot be removed or implanted using behavior modification. The gamemaster determines whether a particular negative quality can be treated or implanted this way, but examples of ones that typically work include: Addiction, Codeblock, Combat Paralysis, Elf Poser, Ork Poser, and Simsense Vertigo (p. 93, *SR4A*). The Karma Cost for removing a Negative quality must still be paid.

If the test fails, the subject's behavior remains unmodified. If the test suffers a critical glitch, unexpected side effects occur and the negative quality is made worse or altered significantly in some way determined by the gamemaster. Since behavior modification is not hidden, no test is needed to detect it in the subject. Behavior modification can be reversed with another behavior modification test.

## SKILLWARE: SKILLS ON DEMAND

Skillware is a spin-off technology from simsense, taking the application of ASIST and going beyond the sensory regions of the brain, stimulating and manipulating the cerebral cortex and cerebellum in order to enable knowledge and skills the user does not typically have. The spread of skillware has reshaped social approaches to education and labor, unfortunately not always for the better. There are three types of skillware recordings: linguasofts, knowsofts, and activesofts.

### LINGUASOFTS

Linguasofts are ASIST recordings of language processing, reading, and speech. The recordings focus on stimulating the left hemisphere of the metahuman brain, where most understanding and formation of language occurs. In essence, linguasofts are real-time translation systems, intercepting activity in the language centers of the brain and inserting new signals that allow a user to understand, read, and speak in languages they otherwise do not comprehend. The typical linguasoft is actually a mixed recording of hundreds of polylingual speakers, which not only assists in rounding out the breadth of a language the linguasoft covers, but also allows users with different native language backgrounds to use the same linguasoft.

### KNOWSOFTS

Knowsofts focus on the cerebral cortex, the complex neural pathways that associate memory with learning and knowledge. When knowsofts are recorded, skilled individuals are deeply tested on a particular topic of knowledge and the recording focuses on the information retrieved by their memories. This information is recorded and encoded into "chunks,"


compartmentalized pieces of information that a knowsoft loads into the short term memory of the user. When the knowsoft user attempts to recall a knowledge skill they do not possess, their brain retrieves these pieces from short term memory and processes them, much like remembering a commlink number one has just seen. Since the information is not processed in long-term memory, the user does not learn the skill. When they remove the knowsoft, the skill will fade from their short term memory in about thirty seconds.

## ACTIVESOFTS

Activesofts trigger activity not only in the metahuman brain, but also the neuromuscular system. For this reason, activesofts also require skillwires (p. 342, *SR4A*), neuromuscular controllers that activate muscle memory in conjunction with the ASIST signals activating brain activity. Early attempts to impart active skills to a user through just the neuromuscular control system produced poor results because the brain rejected the body movements it didn't understand, causing the skills to be imprecise. By introducing ASIST signals that manipulated the cerebellum and cerebral motor cortex, the brain understood the neuromuscular signals and cooperated, leading to fine motor control and the ability to reproduce skills accurately.

## SKILL NETWORKING

Wireless simsense also allows for skill networking, where one skillwired person can use the wireless network to share a skill program with another wireless-capable skillwired person. The neuromuscular signals that would usually be sent to their body are instead transmitted to the second person's skillwires via commlink and sim module. Both characters must be equipped with skillwires and their personas must be subscribed to each other. A programmed skill that is being shared may not be used by the sharing character.

## THE CHIPPED WORKFORCE

Going back as far as the assembly line, technological revolutions have caused great upheaval in the way labor operates in the world. The appearance of skillware has been the most profound change to the workforce since the development of the Internet in the last century. The Sixth World has only barely begun to explore the benefits and hidden risks of skillware on the labor pool, but already it has reshaped the way people work across the globe.

### The End of Unskilled Labor

By the 2070s, most manual labor has been replaced by robotics and drones. Even though activesofts would allow unskilled workers to become proficient in skilled manual labor, machines have shown to out-perform chipped metahuman workers in terms of efficiency. However, chipped labor can still be found in many computer-assisted, white collar fields where a metahuman touch is still preferred.

Activesofts and knowsofts have greatly impacted the healthcare industry, enabling naturally unskilled labor to perform as nurses, caretakers, and pharmacists simply by slotting chips. Insurance agents, accountants, and sales representatives have also been similarly transformed, instantly able to learn new business skills and master new product lines. In these and similar fields, expensive and time-consuming training and education programs have been completely replaced by mass-produced skillsofts.

### The Rise of Creative Labor

The commonplace use of skillsofts to impart basic skills to unskilled workers has had the side effect of increasing the value of creative labor, workers who can think outside the box. Anyone can slot a chip and possess the skills to do a job, but a skillsoft does not teach a person to apply those skills in a creative fashion to achieve new results. As a result, high-paying jobs do not necessarily rest on mastering a particular skill, but in demonstrating how you can uniquely apply that skill. Innovation drives this new, valued workforce and has become the currency in the global labor pool. This is hardly news to most shadowrunners; corporate extractions have long revolved around employees who possessed unique insights that made them valuable to competitors.

### The Global Office

Linguasofts have eliminated the biggest barrier to international business by enabling workers to seamlessly shift languages as soon as they land in a new nation. The new global worker will also usually be fitted with knowsofts (and sometimes even activesofts) for local customs, so they can avoid committing a *faux pas* while representing their company. As a result, there is an entire class of workers who have no "home office" and instead are transient, relying on skillsofts and the wireless Matrix to conduct business wherever necessity takes them.

### Wageslavery

While employers reap the benefits of skillware, such as low costs and quick training, chipped employees suffer from detachment and a lack of upward mobility. Most chipped workers have little or no pride in their work, a side effect of performing their jobs with skills they do not naturally possess. They perform their jobs virtually on autopilot, with a wage or salary being their only real reward. The lack of personal fulfillment has led to numerous side effects, including widespread depression and high addiction and suicide rates among chipped workers.

Additionally, since chipped skills are not learned, advancement and upward mobility are limited for chipped workers. Corporations have done away with training programs in favor of skillsofts, but that leaves a worker with no marketable skills once the chip is removed. As a result, most chipped workers are bound to their employer, unable to market themselves to a competitor.

### Neo-Luddites

The megacorporations have virtually crushed labor unions, leaving chipped labor with few options for collectively voicing their frustration. But the ease with which the global marketplace can shift and suddenly leave thousands of unskilled unemployed has riled up the anger of chipped labor, and the wireless Matrix has begun to give a voice to these workers around the world. The first major example of this new movement might be the organization known as 9x9 in Hong Kong, which appears to be a multi-faceted terrorist organization fueled by labor imbalances and class strife. 9x9 strikes out at corporate manufacturing and transportation in Hong Kong, similar to the way the nineteenth century Luddites destroyed the mechanized looms of the Industrial Revolution.

## SKILL SERVICE PROVIDERS

Wireless ASIST has changed the way people typically receive a skillsoft, replacing the pre-packaged retail chips of old with wireless downloads straight into the user's commlink. Now a customer can purchase a skill when they need it, as opposed to making a run to the store or waiting for the chip to be shipped to their home. A number of skill service providers have appeared on the scene, companies that sell these direct download skillsofts. While they are all selling virtually the same product, these competitors have differentiated each other in their target consumers and level of quality. It is worth noting that all major skill service providers require a valid SIN to create an account and begin downloading skills.

### WorkShop (Renraku)

Renraku's WorkShop is the big player in the realm of skill service providers. WorkShop was founded as an incubator startup in 2065, rumored to be based on technology researched at (or acquired from) the Renraku Arcology. As the fledging wireless ASIST networks went up, WorkShop was in place to immediately start delivering wireless skillsoft downloads. Since then, WorkShop has solidified its majority control of the marketplace by offering a wide selection of skillsofts in a varying degree of skill level (most linguasofts and knowsofts up to Rating 5 and activesofts up to Rating 4). Skillsofts can be purchased individually, or subscribers can pay an annual membership fee for frequent-user discounts, package deals, and other promotions.

### Kolkota Integrated Talent and Technologies

India's only AA corporation, KITT has made significant inroads into wireless skillsoft distribution, particularly in corporate training. KITT has focused on low-rating skills (Rating 1–3) geared towards the business world, promising to show companies how they can transform their workforce through skillsoft downloads. In addition, KITT has started up a skill networking service, where business customers can have a trained KITT professional remotely network a skill from across the globe, enabling high-rating skills on demand for contracted periods of time.

### Luxe (Spinrad Industries)

In Spinrad Industries' fierce fight to become a major contender again in the world of metahuman enhancement, they have added Luxe, a skill service provider specializing in "designer skills." Luxe sells high rating skillsofts (Rating 3–5 knowsofts and linguasofts, and Rating 3–4 activesofts), many of them featuring skills recorded from so-called skillebrities, popular figures known for their skill in a certain field. Luxe is also known for selling skillsofts with many options (*Program Options,* p. 114), tailoring them to the buyer's desires. Though Luxe's market share is still small, there is a lot of buzz around this skill provider, buzz that Johnny Spinrad hopes to ride to high profits.

### Lifeline (Horizon Group)

Lifeline is Horizon's new effort in the field of wireless skill downloads. Though its collection of activesofts is anemic compared to Renraku's WorkShop, Lifeline has a vast collection of linguasofts and knowsofts in all ratings. More importantly, a buyer can opt for the Lifeline program option (p. 114), which connects their linguasoft or knowsoft to Horizon's specialized online search engine, greatly expanding its potential and adaptability. Horizon has also been pitching business solutions intended to assist organizations in establishing and maintaining internal skill networking methods, which makes some wonder if Horizon already uses these techniques extensively in-house.


Glitch was an insect.

He loved how the world always seemed so large from his bug's eye view. He hated how it made him feel vulnerable. As he climbed up the wall, he fought down a sudden shiver—the feeling of so many gecko tips catching and releasing on his multiple legs gave him the willies. He could feel one of his legs cramping up—the micro-servos on one of the drone's legs must be acting up again.

He reached his destination: a small vent grate that loomed like a vast cavern mouth. He skittered inside, dragging a thin fiberoptic cable with him. From there it was another twenty minutes of crawling through vents, even passing through the wired mesh of the facility's Faraday cage.

Finally he reached the darkened lab. He scurried across it, taking a dangerous path across open space rather than sticking to the walls—he was afraid he had misjudged the distance, and his reel of fiberoptic might run short. He was halfway to his destination when the ground began to shake. He froze and peered through the sensors, but was suddenly blinded by a powerful light. His virtual eyes recovered from the glare just in time to see a large boot come stomping down right next to him. His body screamed to move, certain that he was about to be stepped on.

But the footsteps receded across the room, taking the light with them—a guard, making the rounds. Close call. One misstep and his drone body would've been crushed, dumping him from the Matrix and spoiling the run.

He skittered on, taking another few minutes to locate the object of his search: a fiberoptic cable that he hoped led directly to the research nexus he planned to penetrate. His insectoid pincers gripped the cable, applying the optical tap. It bent the cable, capturing a minor amount of the light signals passing through it, without disrupting the connection. The tap linked the cable to the one Glitch had dragged in from outside.

He took a deep breath, jumped out of the drone, and dove into the cable. His persona materialized before a set of Roman ruins—the nexus's login gateway—and immediately assaulted the node's defenses, scanning for an exploitable weakness. He kept his hacking tools up to date, and in just a few seconds he had found a software vulnerability, taking advantage of it to bypass the firewall and acquire user privileges. He passed between the tall pillars, entering a large coliseum. A pair of large lions sauntered past, not seeing to see him. Yet.

From there, it took him only a few minutes to survey the lab's latest research—cutting-edge commlink design. He spent a few minutes admiring the handiwork and design principles that would go into the commlinks hitting the market in 5 year's time. His inner geek smiled. Then he logged out, cut the tap, jumped back into the microdrone, and headed out. He took nothing with him.

Sometimes, the thrill of the hack was just knowing that you could.

## COMMLINKS, MODULES, AND NEXI

The following commlinks and nodes follow all of the rules given in both this book and *Shadowrun, Twentieth Anniversary Edition*. They may be customized according to rules on p. 228, *SR4A*. Any accessories described in this section are plug-and-play or otherwise easy to add/install (modifications requiring a skill test are listed under *Commlink Modifications,* p. 196).

Note that the electronics options presented on p. 58, *Arsenal,* are also available for commlinks and nodes.

### Cryptosense Module

This module allows the user to interpret sensory data she isn't wired for, such as thermographic sense, ultrasound sense, electroreception, sonar, etc. See *Cryptosense Sculpting*, p. 72.

### Disposable Commlink

This cheap mass-produced commlink is designed for temporary use and anonymity. These commlinks come with a short-term MSP basic service plan and commcode, good for one week.

### Fetch Module

This plug-in processor module is dedicated to running a specific agent—the so-called "Fetch." Since the Fetch is run on the dedicated module, it does not count towards the controlling persona's processor load (but it does take a subscription when run autonomously). The Fetch is equipped with a Browse program of equal rating and a personafix program (both also run on the processor). The personafix gives the Fetch a distinct personality, often based on historical characters, trideo actors, anime characters, etc. Fetch modules may not be loaded with other software or data. For the Fetch to operate autonomously, the commlink must remain on and have an active Matrix connection (the module does not have its own wireless link).

### Nexi

Nexi are nodes designed for more users and traffic than standard nodes like commlinks and home terminals (see *Nexi,* p. 50). Nexi can be purchased by their individual component costs, given below (Signal is normal cost), or one of the pre-packaged nexi may be chosen. Most nexi are the size of a desktop computer tower or larger—too large to carry comfortably in place of a commlink, but possible to pull on a cart, load onto a drone, or carry in a vehicle.

**Renraku Hotspot:** Perfect for Matrix cafes, public terminals, and other place where you need to provide Matrix access for a group of people.

**Evo Mobile Terminus:** The Terminus is intended to provide a field nexus in situations where one is needed in an emergency: conflict-zones, disaster areas, media spectacles, etc. The Terminus is commonly found in mobile command posts and media vans.

**Renraku Retailer Hub:** Intended for use by the staff of small retail stores or the departments of larger outlets, this hub limits the Signal for privacy and provides slightly better security.

**NeoNET Office Genie:** Manufactured for small business office environments (or departments in larger offices), the genie provides an access point for up to 30 employees.

**MCT Sentinel:** This security nexus provides an access point for security hackers and spiders, and is often used as a chokepoint for secure networks.

### Nonstandard Wireless Link

Similar to the wireless adapter (p. 50), this plug-in radio uses non-standard radio frequencies (frequencies typically reserved for other uses, and not scanned by nodes seeking to detect other wireless devices). In game terms, this raises the threshold for detecting the wireless node by 1.

### Response Enhancer

This plug-in device radically improves a persona's command channels, boosting its Matrix Initiative by its rating.

## COMMLINK MODIFICATIONS

Commlinks and other electronic devices may be modified by a character without Hardware skill, using the rules for gear modification found on p. 126, Arsenal.

Commlinks are considered to have 4 available modification slots. In addition to the mods noted below, the following options listed under *Weapon Modifications* on pp. 148–153, *Arsenal,* may also be applied to electronics: Ceramic/Plasteel Components, Chameleon Coating, Extreme Environment Mod, Gecko Grip, Metahuman Customization, Propulsion System, Skinlink, and Tracker.

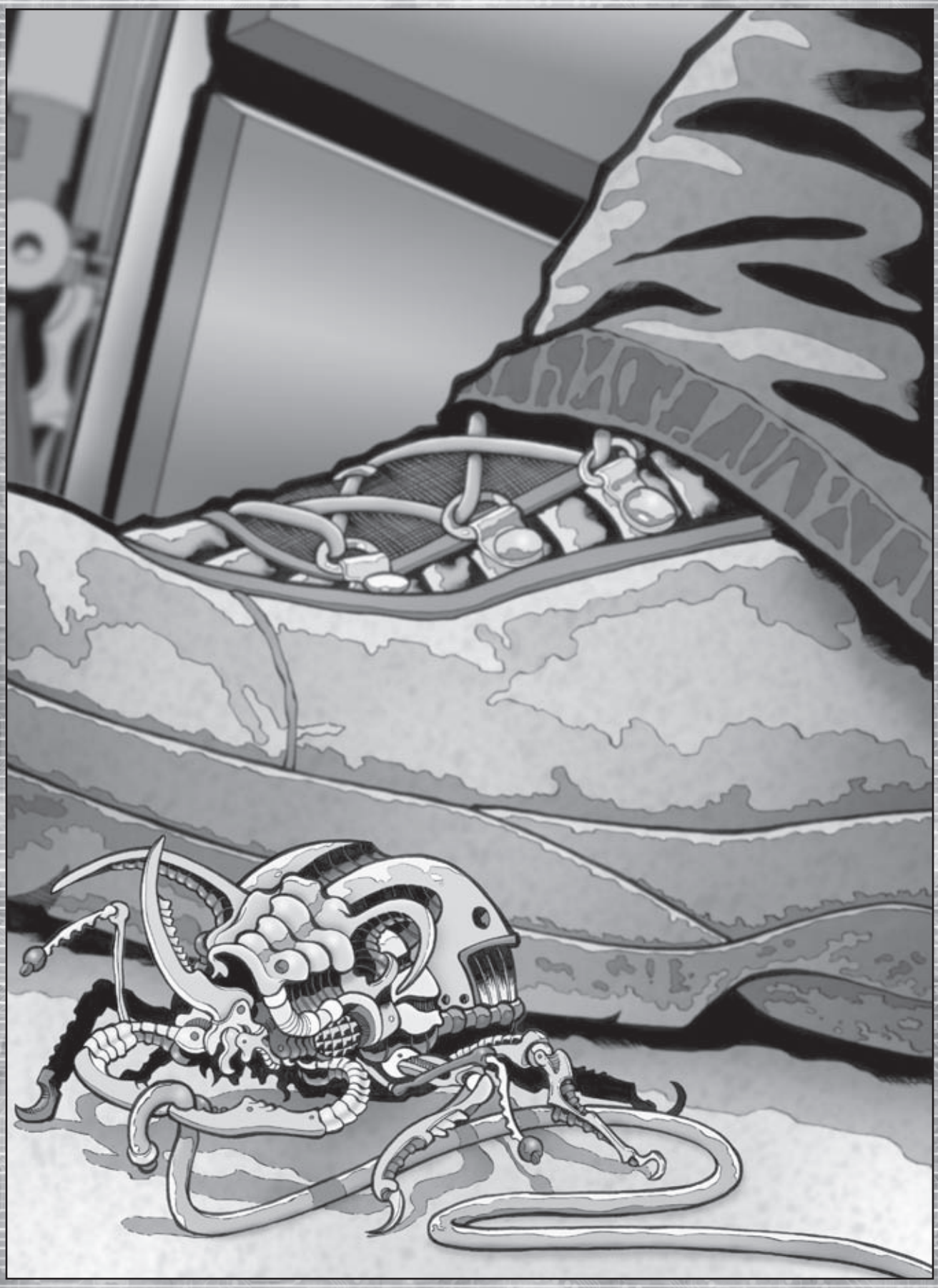
### Armor Case

This mod encases the commlink in an armored case for protection against gunfire, physical attacks, and accidents. Each point of rating serves as 1 point of both Ballistic and Impact armor.

### Biometric Lock

This mod incorporates a biometric lock into the device (see *Biometrics,* p. 263, *SR4A*), so that only someone with an appropriate characteristic can access the device. This lock may be further custom-

| Commlinks and Modules | Response | Signal | System | Firewall | Availability | Cost |
|---|---|---|---|---|---|---|
| Cryptosense Module | — | — | — | — | 8 | 1,000¥ |
| Disposable Commlink | 1 | 3 | 2 | 1 | — | 300¥ |
| Fetch Module (Rating 1–3) | 2 | — | 3 | — | Rating x 3 | Rating x 2,000¥ |
| Fetch Module (Rating 4–6) | 2 | — | 6 | — | Rating x 4 | Rating x 4,000¥ |
| Nonstandard Wireless Link (Rating 1–6) | — | Rating | — | — | 6R | Signal Rating x 500¥ |
| Response Enhancer (Rating 1–6) | — | — | — | — | Rating x 4 | Rating x 2,000¥ |



ized with any of the anti-tamper mods listed under *Advanced Safety* on pp. 148–149, Arsenal, with the exception of the immobilizer.

### Customized Interface

This modification tweaks the simsense channels and control options to work especially well with one specific character. That character receives a +1 bonus to Matrix Initiative. Anyone else using that interface suffers a –1 Matrix Initiative bonus.

### Hardening

Hardening protects against EMP attacks, as noted on p. 58, *Arsenal.*

### Optimization

This modification optimizes the device's processor and components to enhance one particular program, applying a +1 dice pool modifier for all tests using that software. Each device may only be optimized once.

### Self-destruct

As described on p. 58, *Arsenal.*

### Simsense Accelerator

This state-of-the-art mod increases the speed at which simsense signals are transmitted between the commlink and a persona controlled via hot-sim VR. It increases a VR-using character's Matrix Initiative Passes by 1. It does not boost Matrix Initiative in cold-sim VR or AR. It is compatible with simsense booster cyberware (so a hacker in hot sim with a simsense accelerator and simsense booster cyberware has 5 Initiative Passes). Initiative Passes; this is an exception to the rule that normally limits IPs to 4).

## DRONES

These drones follow all of the standard rules given for drone in *SR4A* and *Arsenal.*

**MILITARY-GRADE HARDWARE**

Though we do not offer Availability and Costs for Response and Signal components at a Rating higher than 6, this does not mean that such components do not exist. High Response components do exist in military and elite corporate circles, and occasionally even the shadows, but they are highly-protected and valued, and not easily acquired. High Signal radio transceivers are easier to acquire, being available commercially with the right licenses, but are typically much larger units of no use to a mobile hacker. Ultimately it is the gamemaster's choice whether to allow such items in her game, though they should be expensive and difficult to obtain, possibly being the focal point of an entire shadowrun.

Urgent Message...

### Micro-Tapper Bug

This micro crawler is designed to seek out fiberoptic lines and tap them with a built-in optical tap (p. 199), and either opening a wireless connection back to the rigger, or connect a dragged fiberoptic cable leading back to the rigger, allowing a remote tap.

### Repeater Drone

This flying mini-drone comes equipped with a built-in laser transceiver (Rating 3), directional antenna (Rating 4), and a radio frequency repeater to extend the Signal range of linked devices by its own Signal rating of 4.

### Roving Hub

This medium wheeled drone carries an Evo Mobile Terminus nexus (p. 196), allowing a Matrix access point to be established for multiple users almost anywhere.

| Nexus Hardware/Software | Availability | Cost |
|---|---|---|
| Response (Rating 1–3) | Rating x 4 | Rating x processor limit x 50¥ |
| Response (Rating 4–6) | Rating x 4 | Rating x processor limit x 100¥ |
| System (Rating 1–3) | persona limit ÷ 5 | Rating x persona limit x 25¥ |
| System (Rating 4–6) | persona limit ÷ 2 | Rating x persona limit x 50¥ |
| Firewall (Rating 1–3) | processor limit ÷ 10 | Rating x processor limit x 25¥ |
| Firewall (Rating 4–6) | processor limit ÷ 5 | Rating x processor limit x 50¥ |

**Note:** The processor limit minimum is 10, maximum is 50.

| Pre-packaged Nexi | Response | Signal | System | Firewall | Persona Limit | Processor Limit | Availability | Cost |
|---|---|---|---|---|---|---|---|---|
| Renraku Hotspot | 3 | 3 | 3 | 2 | 10 | 20 | 8 | 5,000¥ |
| Evo Mobile Terminus | 3 | 5 | 3 | 3 | 20 | 50 | 14 | 10,000¥ |
| Renraku Retailer Hub | 2 | 2 | 3 | 4 | 10 | 20 | 8 | 6,000¥ |
| NeoNET Office Genie | 3 | 2 | 4 | 3 | 30 | 50 | 8 | 15,000¥ |
| MCT Sentinel | 4 | 4 | 3 | 5 | 10 | 50 | 16 | 30,000¥ |

## ELECTRONICS

Electronics follow all of the normal rules given for electronics in *Shadowrun, Twentieth Anniversary Edition.*

### Chemical Seal

This temporary spray-on seal provides complete protection for commlinks and other electronics against water and other liquids. It is not effective against acids, however. Even fiberoptic jackpoints are protected. The seal lasts for 24 hours. The sealant sprayer is good for 10 applications.

### Datalock Module

This plug-and-play hardware module is used to store information in a secure format from which it cannot be copied. Data may be read, added to, and erased on the module only if you possess the encryption key (or break the encryption). Datalock modules are common devices used by Johnsons when dealing with runners; the module is loaded with information on the run, so that runners may plug it into their commlinks and access it, and then return it to the Johnson after the run. Datalock modules also features a time-erase function, so that carried data is auto-erased after a set time period.

### Directional Antenna

This device focuses a radio signal along a straight unidirectional path, rather than in all directions. It is used to minimize signal scatter and provide privacy against potential eavesdroppers. The antenna is shaped like a pistol grip with a parabolic dish and plugs into commlinks or other nodes. Add 2 to the antenna's rating for determining Signal range, but it can only communicate with nodes in the path of the radio beam.

### Fiberoptic Cable

This cable is used to establish a wired connection between two devices.

### Laser Link

This device allows an attached node to communicate with other laser-equipped nodes (see *Beam Links,* p. 51). Laser links require line of sight, and may be hampered by smoke or fog (reduce Signal by the Visibility modifier). Laser links are immune to radio-frequency jamming. (The laser link on p. 58, *Arsenal,* is simply a Rating 2 laser link.)

### Mesh Tags

These RFID tags are designed to be spread en masse over a large area (spread from drones, airburst from mortars, etc.) so they may act as micro-routers and create an ad-hoc mesh network in static or dead zones. They have a Signal rating of 2.

### Microwave Link

Similar to a laser link, except this device emits microwaves for communication.

### Optical Tap

This device is used to tap fiberoptic lines, so that data transferring over them may be intercepted. A clip-on coupler places a micro-bend in the cable so that light signals may be captured (without interrupting the signal). This requires a Hardware + Logic (2) Test. The tapper can then perform an Intercept Traffic operation (p. 230, *SR4A*).

### PAB Units

Programmable ASIST Biofeedback units, used for brainwashing, are detailed on p. 189.

### Simdeck

Larger than a standard sim module (laptop or desktop-sized), simdecks are also much better than sim module's when it comes to experiencing simsense. See *Playback Gear,* p. 187.

| Modification | Slots | Threshold | Tools | Cost | Availability | Special Skill |
|---|---|---|---|---|---|---|
| Armor (Rating 1–10) | 1 | 4 | Kit | Rating x 50¥ | 8 | Armorer |
| Biometric Lock | 1 | 8 | Kit | 150¥ | 4 | — |
| Customized Interface | 1 | 8 | Kit | 250¥ | 6 | Software |
| Hardening (Rating 1–6) | 1 | 12 | Shop | Rating x 25¥ | 4 | — |
| Optimization | 1 | 12 | Shop | 500¥ | 6 | Software |
| Self-destruct | | | | | | |
| Localized | 2 | 12 | Shop | 2,000¥ | 16F | Demolitions |
| Area Effect | 2 | 12 | Shop | 10,000¥ | 20F | Demolitions |
| Simsense Accelerator | 2 | 12 | Shop | 15,000¥ | 14 | — |

| Drone | Handling | Accel | Speed | Pilot | Body | Armor | Sensor | Avail | Cost |
|---|---|---|---|---|---|---|---|---|---|
| Micro-Tapper Bug | +1 | 2/10 | 10 | 3 | 0 | 0 | 1 | 8 | 1,000¥ |
| Repeater Drone | +1 | 3/15 | 15 | 3 | 1 | 0 | 2 | 6 | 3,000¥ |
| Roving Hub | 0 | 10/25 | 75 | 3 | 3 | 2 | 3 | 6 | 13,000¥ |

### Skinweb Array

This metal-weave antenna is worn on the skin (back, chest, limbs) underneath the clothing. It improves transmission and reception, providing a +1 ECCM bonus against jamming and lessening the penalty for being in a static zone by 1.

### Wireless Adapter

This device is a radio transceiver that plugs into the terminus of an optical cable or the optical jack of another device, allowing it to act as a wireless device with a Signal rating of 3.

## NANOTECH

The following nanotech gear follows the rules for nanotech given in *Augmentation*.

### Hacker Nanites

**Vector:** Injection
**Speed:** 1 minute
**Penetration:** 0
**Power:** 8
**Effect:** See description

These variants of Intruder nanites (p. 116, *Augmentation*) are designed to seek out cyberware systems and infect them. If the implant's wireless has been disabled, the hackers will enable it. If the implant has been slaved to another device, that slaved connection is killed. Instead, the hacker nanites slave the cyberware to the hacker who deployed them, giving that hacker control over the implant. Hacker nanites follow the rules for weaponized nanotech given on p. 115, *Augmentation*.

### Nanomemory

Nanomemory comes in the form of a decorative paste, makeup, skinpaint, temporary tattoos and other fashion products. Its real purpose, however, is to serve as a temporary and worn source of computer memory storage. Highly popular with technomancers, who lack data storage capabilities in their biological nodes, nanomemory allows them to store data on their skin. Nanomemory has a Signal Rating of 0. One application last for 24 hours.

## SECURITY

Faraday cages and wireless negating materials are discussed on p. 62; passkeys are detailed on p. 64.

## SERVICES

These are Matrix services that runners may buy.

| Electronics | Availability | Cost |
|---|---|---|
| Chemical Seal | 4 | 200¥ |
| Datalock Module | 6R | 50¥ + Encryption Cost |
| Directional Antenna (Rating 1–6) | 4 | Rating x 25¥ |
| Fiberoptic Cable | — | 5¥ per meter |
| Laser Link (Rating 1–6) | — | Rating x 25¥ |
| Mesh Tags | — | 2¥ |
| Microwave Link (Rating 1–8) | 8 | Rating x 200¥ |
| Optical Tap | 8R | 100¥ |
| Simdeck | — | 1,000¥+ |
| Skinweb Array | 10 | 200¥ |
| Wireless Adapter | — | 150¥ |

| PAB Units | Device Rating | Availability | Cost |
|---|---|---|---|
| Sony 800AL Field PAB Unit | 1 | 14R | 6,000¥ |
| DocWagon Cleansweep | 2 | 14R | 8,000¥ |
| MCT MemEdit III Suite | 3 | 14R | 10,000¥ |
| Interneurox G-Series Memory Master | 4 | 16R | 13,000¥ |
| Transys-Neuronet MES Grand | 5 | 18F | 16,000¥ |
| Renraku MR-X ASIST Reprogrammer | 6 | 20F | 20,000¥ |

| Nanotech | Availability | Cost |
|---|---|---|
| Hacker Nanites | 10F | Rating x 1,000¥ |
| Nanomemory | — | 200¥ |

## HACKER SERVICES

See *Buying a Better Hacker,* p. 93.

## MSP SERVICES

Matrix service providers not only provide commcodes but are also the reliable backbone of the Matrix, providing public access points, satellite networks, data storage, and much more.

A High lifestyle or better automatically grants access to Premium services. Purchased individually, one has to pay 1 to 10 nuyen per service in the Basic range, Advanced services cost 5 to 20 nuyen, and Premium services range from 50 to 100 nuyen. A valid bank account is needed to purchase Matrix services from most MSPs, though a few will work on a credstick-to-credstick basis.

### Basic Services

Basic services include access to wireless access points in a country, one remote data storage location of unlimited size, and up to four commcodes. Furthermore a remotely run Rating 1 agent with Browse and Edit programs (Rating 1) is available. Basic Matrix services are included with a Low lifestyle.

### Advanced Services

Advanced services include all the features of basic service. In addition, worldwide access to wireless access points is granted, along with the right to connect to geostationary communication satellites and six additional commcodes. The agent service is extended to a remote Rating 2 agent

| Wireless Negation | Availability | Cost |
|---|---|---|
| Faraday Cage, per $m^3$ | 4 | 100¥ |
| Wireless Negating Paint, per can (30 $m^2$ coverage) | Rating | Rating x 20¥ |
| Wireless Negating Wallpaper, per 10 $m^2$ strip | Rating | Rating x 5¥ |
| **Passkeys** | | |
| Standard Passkey | 4 | 100¥ |
| Nanotech Passkey | 12 | 1,200¥ |
| Alchemical Passkey | 16 | 2,100¥ |
| Standard Passkey System | 4 | 15,000¥ |
| Nanotech Passkey System | 12 | 32,000¥ |
| Alchemical Passkey System | 16 | 110,000¥ |

| Hacker Services | Availability | Cost |
|---|---|---|
| Hacking a passcode | 12R | Hacking skill x 500¥ |
| Setting up a hidden account | 16F | Hacking skill x 1,000¥ |
| Copying a certified credstick | 24F | Half the amount (in real nuyen) |
| Spoofing a lifestyle (1 month) | 16F | Half cost of lifestyle for 1 month |
| Jacking a vehicle or drone | 8R | Hacking skill x 200¥ |
| DOS attack on an individual (1 hour) | 8F | Hacking skill x 200¥ |
| Tracing a datatrail | 6R | Hacking skill x 100¥ |
| Renting a botnet | 10F | Number of bots x Cost of bots x 0.5¥ an hour |
| Buying a botnet | 15F | Number of bots x Cost of bots x 5¥ |
| Anonymizing proxy service | 4 | Number of reroutes x 10¥ per day |
| Anonymized commcode (calls/messaging) | 4 | Number of reroutes x 5¥ per day |
| One-time disposable commcode | 4 | 10¥ |
| Numbered credit account | 4R | 100¥/month |
| One-time disposable credit account | 6R | 10% of the deposited amount |
| Escrow service | 8R | 10% of the deposited amount |

| MSPs | Availability | Cost |
|---|---|---|
| Basic Services | — | 25¥ per month |
| Advanced Services | — | 50¥ per month |
| Premium Services | — | 100¥ per month |

with Rating 2 programs. The remote data storage is secured by regular back-ups to other remote sites. Advanced Matrix services come with Medium lifestyle.

### Premium Services

Premium services grant all the features from basic and advanced services. On top of that, access to low-earth orbit satellites is included, as well as an anonymization service for an unlimited number of commcodes. Data storage and two back-ups are located in a protected security facility (Firewall 4, Analyze 4, IC Rating 3).

## SOFTWARE

These programs and program options are described in the *Software* chapter, p. 106, and are included here again for easy reference. Unrestricted agents (see *To Mook or not to Mook* sidebar) are on p. 101, Telematics Infrastructure software on p. 62, pre-packaged IC can be found on p. 71, and reality amplifiers on p. 188.

| Mook | Availability Modifier | Cost Multiplier |
|---|---|---|
| Unrestricted Agent | +2 | 1.2 |

| ARE Software | Availability | Cost |
|---|---|---|
| Body Shop | — | 50-500¥ + 10-100¥/month |
| Glyphs | — | 20-5,000¥ |
| Negator | 4 | 100¥ |
| Ractives | 4 | 1,000¥ + 200¥/month |
| Scentsasion | — | 50¥ |

| Program Option Type | Availability (per option) | Cost (per option) |
|---|---|---|
| General* | +1 | +(Rating x 100¥)† |
| Biofeedback | +12R | +(Rating x 500¥) |
| Psychotropic | +16R | +(Rating x 1,000¥) |
| Hacking | +2R | +(Rating x 750¥)† |
| Simsense | +2 | +(Rating x 1,000¥)† |
| Addictive | x2 | +(Rating x 1,000¥) |

| Software Coding | Availability | Cost |
|---|---|---|
| Software Programming Suite (Rating 1–5) | 6 | Rating x 1,000¥ |
| Programming Environment Access | 8 | 100¥ per day |

| Tactical Software | Availability | Cost |
|---|---|---|
| Tacsoft (Rating 1–4) | Rating x 5 | Rating x 3,000¥ |

| Program Packages | Availability | Cost |
|---|---|---|
| Eastern-Tiger Palladium | 6R | 6,640¥ |
| Eurosoft Clavicula | 10R | 4,700¥ |
| FTL Matrixware Net Wizard | — | 480¥ |
| FTL Matrixware Power Suite | — | 1,240¥ |
| Pocket Hacker | 10F | 4,920¥ |
| Singularity Seeker | 4 | 8,200¥ |

* Registration and Copy Protection are included by default in all legal software (at no extra Availability/Cost).
† Options without a rating are considered Rating 3 for cost purposes.

| Software Suites | Availability | Cost |
|---|---|---|
| Homewrecker | 12F | 6,000¥ |
| Iris Antivirus | — | 1,500¥ |
| Shamus | 6F | 5,500¥ |

| Skillsoft Clusters | Availability | Cost |
|---|---|---|
| DocWagon Paramedic | 6 | 44,800¥ |
| Knight Errant Self-Defence | 8 | 48,000¥ |
| Manadyne Archmage | 8 | 28,800¥ |
| Mitsuhama Home Mechanic | 8 | 44,800¥ |
| Whiskey Noir | 8 | 46,400¥ |

| Telematics Infrastructure Software | Availability | Cost |
|---|---|---|
| Telematics Infrastructure (Rating 1–3) | (Rating x 2)R | Rating x 400¥ |
| Telematics Infrastructure (Rating 4–6) | (Rating x 2)R | Rating x 800¥ |

| Reality Amplifiers | Availability | Cost |
|---|---|---|
| Reality Amplifier Software/Chip | 14R | 500¥ |

| Pre-Packaged IC | Availability | Cost (up to Rating 3) | Cost (up t o Rating 6) |
|---|---|---|---|
| Baby Swarm | (Rating x 3)R | Rating x 3,825¥ | Rating x 8,100¥ |
| Encryption Prescription | (Rating x 3) | Rating x 945¥ | Rating x 2,340¥ |
| Ixcuiname | (Rating x 3)R | Rating x 3,375¥ | Rating x 5,175¥ |
| Juhseung Saja | (Rating x 3)R | Rating x 2,745¥ | Rating x 5,940¥ |
| MCT Bloodhound | (Rating x 3)R | Rating x 1,395¥ | Rating x 3,240¥ |
| Renraku Oniwaban | (Rating x 3)R | Rating x 2,250¥ | Rating x 4,950¥ |
| Rumpelstiltskin | (Rating x 3)R | Rating x 1,800¥ | Rating x 4,050¥ |
| Singularity Encore | (Rating x 3) | Rating x 900¥ | Rating x 2,250¥ |
| Three Musketeers Suite | (Rating x 3)R | Rating x 4,050¥ | Rating x 9,450¥ |
| Transys Florence | (Rating x 3)R | Rating x 1,350¥ | Rating x 3,150¥ |
| Watanabe Electric Kitsune | (Rating x3) | Rating x 945¥ | Rating x 2,340¥ |

| Malware | Availability | Cost (up to Rating 3) | Cost (up to Rating 6) |
|---|---|---|---|
| Trojan | (Rating x 4)F | Rating x 1,000¥ | Rating x 2,000¥ |
| Virus | (Rating x 3)F | Rating x 500¥ | Rating x 1,000¥ |
| Worm | (Rating x 5)F | Rating x 2,000¥ | Rating x 5,000¥ |

# SAMPLE NODES

## SAMPLE PERIPHERAL NODES

| Device | Response | Signal | System | Firewall |
|---|---|---|---|---|
| AR Glove | 2 | 2 | 1 | 1 |
| Credstick | 2 | 2 | 6 | 6 |
| Fridge | 1 | 3 | 2 | 1 |
| RFID tag | 1 | 1 | 1 | 1 |
| Security Camera | 2 | 3 | 2 | 4 |
| Smartgun | 2 | 1 | 3 | 4 |

## EXAMPLES OF STANDARD NODES

| Node | Response | Signal | System | Firewall |
|---|---|---|---|---|
| Standard Home Telecom | 3 | 3 | 3 | 3 |
| Premium Telecom | 4 | 3 | 4 | 4 |
| Business/Retail Terminal | 3 | 3 | 4 | 4 |
| Public Terminal | 2 | 1 | 2 | 2 |
| Civic/MSP Wireless Access Point | 3 | 6 | 3 | 5 |

## EXAMPLES OF NEXUS NODES

| Nexus | Response | Signal | System | Firewall | Persona Limit | Processor Limit |
|---|---|---|---|---|---|---|
| Small Matrix Cafe | 2 | 3 | 3 | 2 | 9 | 10 |
| Large Matrix Cafe | 3 | 3 | 4 | 2 | 12 | 20 |
| Public Library | 5 | 4 | 4 | 3 | 12 | 50 |
| Online Shop | 3 | 4 | 3 | 4 | 9 | 15 |
| Matrix Backbone Hub | 5 | 0 | 5 | 3 | 15 | 50 |

## ACTIONS NEEDING SUBSCRIPTIONS:

- Accessing a node*
- Command connections to drones and agents
- Encrypted connections†
- Jumped-in rigger connections to a drone
- Slaved connections (p. 59)
- Tacnets (p. 125)
- Using a program on another node

* An agent run on a persona does not take up an extra slot, while an independent agent does

† Only encrypted connections that wouldn't otherwise take up a subscription slot count. For example, an encrypted link to an agent takes up only 1 subscription, not 2.

## ACTIONS HANDLED BY DATA REQUESTS:

- Audio/video communications
- Database access
- File transfers
- Newsfeeds and updates
- Social networking
- Text/graphic messages
- Website requests

## COMMON RIGGER/DRONE TESTS

| Action | Jumped-In Rigger Dice Pool | Autonomous Drone Dice Pool | Remote-Controlled Dice Pool |
|---|---|---|---|
| Initiative | as rigger | Pilot + Response | as rigger |
| Attack | Sensor + Gunnery | Pilot + Targeting | Command + Gunnery |
| Melee Defense | Response + Melee skill | Pilot + Defense | Command + Melee skill |
| Ranged Defense | Response | Response | Command |
| Full Defense | as above + Dodge | as above + Defense | as above + Dodge |
| Damage Resistance | Body + Armor | Body + Armor | Body + Armor |
| Infiltration | Response + Infiltration | Pilot + Covert Ops | Command + Infiltration |
| Maneuvering | Response + Vehicle skill | Pilot + Maneuver | Command + Vehicle skill |
| Perception | Sensor + Perception | Sensor + Clearsight | Sensor + Perception |

## SAMPLE NODES *(CONT.)*

### ADVANCED PROGRAMMING TABLE

| Software | Threshold | Interval |
|---|---|---|
| Agent/IC/Pilot | Rating x 3 | 3 months |
| AR Environment | 12 | 1 month |
| Autosofts | Rating x 2 | 6 months |
| Common Use Programs | Rating | 1 month |
| Firewall | Rating x 2 | 3 months |
| Hacking Programs | Rating x 2 | 1 month |
| Sensor | Rating x 2 | 1 month |
| System | Rating x 2 | 6 months |
| Tactical | Rating x 3 | 6 months |
| **Program Options** | | |
| General | Rating* | 1 month |
| Biofeedback | Rating x 2 | 1 month |
| Psychotropic | Rating x 3 | 3 months |
| Hacking | Rating* | 1 month |
| **Malware** | | |
| Bugs (adding) | 4 | 1 hour |
| Bugs (finding/repairing) | 12† | 1 week |
| Virus | Rating x 4 | 3 months |
| Metamorphic Engine | +6 | +1 month |
| Trojan | Rating x 4 | 3 months |

* Options without a rating are considered Rating 3 for Threshold purposes.
† Subject to gamemaster discretion. If the bug is intentionally added, threshold = net hits x 4.

## SECURITY SCRIPTING

### SCRIPTING

A script can take the form of an actual script, a list of conditions and actions that the IC runs through when acting. For example, a script for the MCT Bloodhound might look like this:

1. Is there an active alert?
   a. If yes, then go to 2.
   b. If no, then go to 5.
2. Has the intruder already been Tracked successfully?
   a. If yes, then stand down.
   b. If no, then go to 3.
3. Perform a Track on the intruder. Go to 4.
4. Does the Track finish successfully?
   a. If yes, notify spider of intruder's location and access ID. End action for this Initiative Pass.
   b. If no, end action for this Initiative Pass.
5. Perform Matrix Perception Test on the icon that has been Analyzed least recently. Go to 6.
6. Is the Analyzed icon an intruder?
   a. If yes, initiate an active alert and End action for this Initiative Pass.
   b. If no, end action for this Initiative Pass.

This format is longer and more involved than a brief description, but reflects the IC's limited decision-making abilities. When using this method of scripting, remember to make sure that every numbered entry can be reached from another (except the first, which is where the IC starts), and that every entry either leads to another entry or ends the IC's turn in the Initiative Pass.

### FORGERY TABLE

| Forgery | Threshold | Interval |
|---|---|---|
| Fake Corpscrip | (Rating x 20) | 1 day |
| Fake Game Credits | (Rating x 16) | 1 hour |
| Fake License | (Rating x 16) | 1 hour |
| Fake National Currency | (Rating x 18) | 1 day |
| Fake Nuyen | (Rating x 24) | 1 day |
| Fake SIN | (Rating x 32) | 1 week |

### PAYDATA STREET COSTS

| Situation | Cost Adjustment |
|---|---|
| Data is damaged, but mostly salvageable | –20% to –50% |
| Data is only available on an obsolete medium | –20% |
| Data is publicly available but obscure | –10% |
| Data is in a Proprietary File Format | +10% |
| Certified data | +50% |
| Sole remaining copy of data | +100% |
| Unique enchantment formula | +200% |
| Nanoschematics | +400% |
| Spirit formula | +400% |

# SECURITY SCRIPTING *(CONT.)*

## VERIFYING PROGRAMS TABLE

| Hits | Information Learned |
|---|---|
| 1 | The nature and type of the program |
| 2 | The program's rating |
| 3 | Existence of program options (+1 per additional hit) including option ratings |
| 4 | Detect code error and bugs |
| 5+ | Manufacturer or programmer (if signed) plus any further information that the program may provide |

## CORRUPTION TABLE

| Threshold | Corrupted Data Task |
|---|---|
| 2 | Corrupt some specific information on a basic commlink |
| 4 | Compromise a criminal dossier in a police database |
| 8 | Impair all copies of a file in a corporate nexus |
| 15 | Corrupt every mention of Aztechnology's secretive board of directors from Jackpoint |
| 20+ | Scramble all SINs with the same biometric data in the Global SIN Registry nexus |

## CRACKING COPY PROTECTION

| Program Type | Threshold (Interval 1 hour) |
|---|---|
| Common | 9 + Rating |
| Hacking | 13 + Rating |
| Agents/IC/Pilot | 13 + Rating |
| System | 10 + Rating |
| Firewall | 13 + Rating |
| Autosoft | 12 + Rating |

## SPOOFING LIFE

| Lifestyle | Threshold |
|---|---|
| Squatter | 2 |
| Low | 4 |
| Middle | 12 |
| High | 48 |
| Luxury | 100+ |
| Hospitalized Standard Care | 15 |
| Hospitalized Intensive Care | 30 |

Urgent Message...

## SAMPLE SPIDERS

Below are some sample spiders that a shadowrunning team may encounter directly or indirectly during a run. Each entry includes a short description and a block of game statistics. These examples, along with the Spider contact (p. 12, *Contacts and Adventures*) can be used "as is," or modified to fit a particular node or setting. The statistics given are only those related to the Matrix; gamemasters should feel free to flesh out these examples with appropriate skills and gear. These examples give stats for humans; spiders of other metatypes should have their attributes adjusted accordingly (p. 4, *Contacts and Adventures*).

**Casual Hacker (Professional Rating 0)**

Casual hackers have read some Matrix sites, done a bit of programming, maybe even jumped into a drone at one point. They are hobbyists or just the unlucky person at the office who was tagged for the job.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 3 | 2 | 2 | 3 | 3 | 3 | 2 | 2 | 6.0 |

**Skills:** Computer 2, Data Search 2, Software 1, Cracking Skill Group 1, Etiquette 3, Pilot Ground Craft 2, Current Events Knowledge 3
**Gear:** Contact lenses (w/ image link), AR gloves, sim module, trodes
**Commlink:** System 2, Response 2, Firewall 2, Signal 3
**Programs:** Analyze 2, Browse 1, Command 1, Edit 1, Encrypt 1
**Matrix Initiative:** 5
**Matrix IP:** 2
**Matrix Condition Monitor:** 9

**Novice (Professional Rating 1)**

These spiders are usually either in or just out of college or an apprenticeship program, or are gifted self-starters. They occasionally make mistakes, either in their configuration or their responses, but they try their best to keep their systems secure.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 3 | 2 | 3 | 2 | 3 | 3 | 4 | 3 | 5.7 |

**Skills:** Computer 3, Data Search 3, Hardware 2, Software 2, Cracking 2, Etiquette 2, Perception 1, Pilot Ground Craft 3, Pilot Aircraft 1
**Gear:** Goggles (w/ image link, smartlink), AR gloves
**Cyberware:** datajack, sim module
**Commlink:** System 3, Response 3, Firewall 3, Signal 4
**Programs:** Analyze 3, Armor 3, Attack 3, Bio-Feedback Filter 2, Browse 3, Command 3, ECCM 2, Edit 3, Encrypt 3, Medic 2, Track 2
**Matrix Initiative:** 6
**Matrix IP:** 2
**Matrix Condition Monitor:** 10

## SAMPLE SPIDERS *(CONT.)*

**Security Technomancer (Professional Rating 2)**

Technomancers are the newest entry on the security scene. Those that specialize in security face prejudice and distrust in addition to hackers and other digital attackers in the course of their duties.

| B | A | R | S | C | I | L | W | ESS | RES |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 3 | 3 | 2 | 4 | 4 | 3 | 4 | 6.0 | 3 |

**Skills:** Electronics Skill Group 3, Cracking Skill Group 3, Compiling 3, Decompiling 2, Registering 2, Etiquette 3, Perception 1, Pilot Ground Craft 3, Pilot Aircraft 2, Gunnery 2
**Living Persona:** System 3, Response 3, Firewall 3, Signal 2
**Complex Forms:** Analyze 3, Armor 1, Attack 3, Bio-Feedback Filter 3, Command 2, Track 3
**Matrix Initiative:** 9
**Matrix IP:** 3
**Condition Monitor:** 10

**Professional Spider (Professional Rating 3)**

These spiders have been professionals for several years. Most of them like the job, and have settled into a confidence that ranges from informality to cockiness.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 3 | 2 | 3 | 2 | 3 | 4 | 4 | 3 | 5.0 |

**Skills:** Computer 4, Data Search 3, Hardware 3, Software 3, Cybercombat 4, Electronic Warfare 3, Hacking 2, Con 2, Etiquette 3, Perception 2, Pilot Aircraft 3, Pilot Ground Craft 3, Gunnery 3
**Cyberware:** Commlink, sim module, datajack, control rig
**Commlink:** System 4, Response 3, Firewall 4, Signal 4
**Programs:** Analyze 4, Armor 4, Attack 3, Blackout 3, Bio-Feedback Filter 4, Browse 3, Command 3, ECCM 3, Edit 2, Encrypt 4, Medic 3, Scan 3, Track 4
**Matrix Initiative:** 7
**Matrix IP:** 2
**Matrix Condition Monitor:** 10

**Security Consultant (Professional Rating 4)**

Security consultants are experts in their field. Some manage the defense of large or sensitive nodes. Others travel from facility to facility, bringing the security procedures up to speed during each visit.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 4.8 |

**Skills:** Electronics Skill Group 4, Cracking Skill Group 4, Con 3, Etiquette 3, Perception 4, Pilot Aircraft 3, Pilot Ground Craft 4, Gunnery 4
**Cyberware:** Commlink, sim module (w/ hot-sim), control rig, datajack
**Commlink:** System 5, Response 4, Firewall 5, Signal 4
**Programs:** Analyze 5, Armor 4, Attack 4, Blackout 4, Bio-Feedback Filter 5, Browse 3, Command 4, ECCM 4, Edit 2, Encrypt 4, Medic 3, Scan 4, Track 4
**Matrix Initiative:** 9
**Matrix IP:** 3
**Matrix Condition Monitor:** 11

**Risk Management Engineer (Professional Rating 5)**

"Risk management engineer" is a corporate euphemism for a digital operative: loyal to the corporation, dedicated to their jobs, and cold as the machines they use. They can protect a target electronically and physically, or completely erase it from the world and the Matrix.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 3 | 3 | 3 | 2 | 4 | 5 | 4 | 5 | 3.9 |

**Skills:** Electronics Skill Group 5, Cracking Skill Group 5, Con 4, Etiquette 3, Perception 4, Pilot Aircraft 4, Pilot Ground Craft 5, Gunnery 5
**Cyberware:** Commlink, sim module (w/ hot-sim), control rig, datajack, encephalon (Rating 1), math SPU
**Commlink:** System 5, Response 5, Firewall 5, Signal 4
**Programs:** Analyze 5, Armor 5, Attack 5, Black Hammer 4, Blackout 4, Bio-Feedback Filter 5, Browse 3, Command 4, ECCM 4, Edit 2, Encrypt 5, Exploit 5, Medic 3, Scan 5, Track 5
**Matrix Initiative:** 11
**Matrix IP:** 3
**Matrix Condition Monitor:** 12

**Matrix Support Specialist (Professional Rating 6)**

In the Unwired Age, electronic security keeps soldiers alive just as much as armor does. These military Matrix specialists cover military operations from the lowliest commando squad all the way up to the largest division. They are prepared to lay down their icons and their lives to complete their mission.

| B | A | R | S | C | I | L | W | ESS |
|---|---|---|---|---|---|---|---|---|
| 4 | 4 | 4 | 3 | 4 | 5 | 5 | 5 | 2.65 |

**Skills:** Electronics Skill Group 5, Cybercombat 6, Electronic Warfare 6, Hacking 5, Con 4, Etiquette 3, Perception 4, Pilot Aircraft 5, Pilot Ground Craft 5, Gunnery 5
**Cyberware:** Commlink, sim module (w/ hot-sim), control rig, datajack, encephalon (Rating 1), math SPU, simsense booster
**Commlink:** System 6, Response 6, Firewall 6, Signal 5
**Programs:** Analyze 6, Armor 6, Attack 6, Black Hammer 5, Blackout 5, Bio-Feedback Filter 6, Browse 3, Command 5, ECCM 5, Edit 2, Encrypt 6, Exploit 6, Medic 5, Scan 6, Sniffer 5, Spoof 4, Stealth 5, Track 6
**Matrix Initiative:** 12
**Matrix IP:** 4
**Matrix Condition Monitor:** 11