Neo Anarchists'
The Guide to
REAL LIFE

NIGEL D. FINDLEY

FASA CORPORATION

Neo-Anarchists' The Guide to REAL LIFE

FASA CORPORATION

TABLE OF CONTENTS

NEO-ANARCHISTS' GUIDE TO REAL LIFE

INTRODUCTION

R eal Life? Why bother? Get the newest SimTech cranial simdeck and dream your troubles away...
—ad copy, circa 2050

T he **Neo-Anarchists' Guide to Real Life** is a supplement to the **Shadowrun** game system. It explores life in the Seattle sprawl through a series of articles reprinted from a variety of popular sources available to the general public of that city in 2053.

Various shadowrunners have annotated these articles with their opinions and additional information they consider to be of interest to the reader. The gamemaster must decide whether to treat these opinions and evaluations, inserted by individuals who may hold a biased view, as valid. The player can only hope to discover the truth before it is too late.

Specific rules information and game mechanics for each subject discussed in the articles appears in a separate **Rules** section. The gamemaster and players should review these new and expanded rules and agree on which, if any, they will add to their game.

Much of the material in this book at least hints at ways to make life *much* more difficult for characters, ways to complicate even the simplest task. Gamemasters may choose to use these complicating factors sparingly, but should definitely use them. **Shadowrun** games usually let the characters—and their players—off *much* too easily....

Some of the material on credsticks presented in this product originally appeared in the **Shadowrun** sourcebook **Sprawl Sites.** Because that product is now out of print and no longer available, we have updated that material and reprinted it here for reference.

This book is compatible with both the original **Shadowrun** rule book (product stock number 7100), and the **Shadowrun, Second Edition,** rules (product stock number 7900) now available. Page references for both versions are given when applicable. The **Shadowrun, Second Edition,** rules are usually abbreviated **SRII**. The **Archetypes and Contacts** book included in the **Shadowrun Second Edition Gamemaster's Screen** is abbreviated **SRIIGM**. Specific **SRII** rules notations in game statistic blocks (as in NPC or Contact listings) appear in {**boldface brackets**}.

WELCOME TO...

SHADOWLAND

"I have taken all knowledge to be my province."
— Francis Bacon, 1592

CATEGORY	GO TO:
Message Base/Mail System	OK
Special Categories/ Topics (SIGS)	OK
Library Archive	OK
Information Base — SPECIAL FEATURES! (Limited Duration Posting)	
ARES Winter Catalog 2052-53 (Annotated)	OK
Rigger Black Book 2053 (Annotated)	OK
North American Compilation (Tried and True!)	OK
Paterson's Paranormal Creatures of Europe (Delayed. but Coming Soon!)	NOT AVAILABLE
London (Annotated)	OK
Real Life Compilation (GO FOR IT!)	OK
Tir Tairngire Data Dump (Under Decryption! Watch for it!)	NOT AVAILABLE
Shadow Technology Compilation (Oh, man, I wet my pants…)	OK

NEO-ANARCHIST GUIDE TO REAL LIFE

Security Blanket (Basic Corp Security, don't ya know)	OK
Fringe of Space (Suborbital and Semiballistic travel)	OK
Killer Accessories (Security with style)	OK
Dressed to Kill (Style with security)	OK
DocWagon™ (Everything you wanted to know and more)	OK
Seattle on 30¥ A Night (Crashing the hard and cheap way)	OK
Guarding the Till (Security detection systems)	OK
Eating Fast and Fearlessly (Fast-food facts)	OK
Home Security (Beyond the "Do Not Disturb" sign)	OK
Sharper Image (Stuff you don't need, but really want)	OK
Unidirectional Datalines (Abridged geek-speak)	OK
You Are Your Credstick (A primer for those who got)	OK

DOWNLOAD ALL?   OK

NOTE FROM CONTROL—Anyone with any knowledge regarding sabotage to this system should contact me ASAP. Censorship will not be tolerated!

FINDING YOUR FEET

No matter where you go, there you are.
—Anonymous late-20th-century proto-physical adept

Seattle. Where elves from Tir Tairngire rub shoulders with Amerindians from the Native American Nations. Where the world's largest corporations set up shop alongside the smallest, leanest, and meanest entrepreneurial start-ups.

Seattle. Where a single city block can sport two dozen world-class restaurants, each featuring a unique style of cuisine.

Seattle. Arguably one of the most exciting cities to visit in the entire world.

But the city's multi-faceted character—the unique aspects that make it so exhilarating—can also make it seem unapproachable. With so much happening, so many ingredients flavoring the melting pot, how can the casual visitor know what to do and see, know what's hot or what's not, or stay out of danger?

To solve this problem, we put together the **Guide to Real Life**. Available free of charge via the telecom of every hotel room in the city, the **Guide to Real Life** is your online guide to the way Seattle thinks.

The **Guide to Real Life** is not a standard tourist guide; it offers no maps, listings of emergency phone numbers, or tourist attractions. Many excellent online sources already exist to provide this information, including our sister publication, the **Seattle Sourcebook**.

Real Life is more like a snapshot of what is current, important, and new in Seattle in any given week.

To produce **Real Life**, our staff combs the magazines, datafaxes, and faxrolls of the city each week, selecting and reprinting articles, ads, columns, and editorials that we believe provide a sense of the city for that week. We do not concentrate on communicating concrete information, though **Real Life** certainly contains many facts. Instead, we attempt to provide a gestalt, as it were, of life in Seattle—at least for any given week, trying all the while to stay as eclectic and open-minded as possible. A fashion article might be framed between two pieces on personal security, or a column on

corporate style might precede a rough-and-tumble piece from a mag for Urban Brawlers. You'll never know exactly what to expect from one week to the next—both in **Real Life** and the city it reflects.

So sit back and take a look. We guarantee that you'll find a handful of useful facts, but you'll also find that many articles simply get you thinking. And if some of that thinking helps you to understand our city better, then we have done our job.

Blake Turner
Editor-in-Chief, Guide to Real Life
Real Life Data Services (A Mitsuhama Company)

>>>>>[Tourist drek. And worse, tourist drek disseminated by Mitsuhama which, as we all know, is something less than open-minded, Blakey's comments to the contrary.

Actually, I know Blakey—we used to punch deck together before he sold out. A competent guy, really, would have been a great asset to Shadowland. But of course MCT, through SDS, offered him a hell of a lot more money than Shadowland could, basically by offering him money in the first place. Shadowland sysops like me get paid by the knowledge that we help scroffy bleeders and street monsters like yourselves to stretch your miserable lives a couple of days longer.

That said, the *Real Life* idea is a good one for tourists, but it's also worthwhile for less—shall we say *official*—visitors to this fine burg. There's something distinctive about Seattle, something that sets it apart from any other location on the continent or around the world. Genuine differences exist between Seattle and Los Angeles, or Atlanta, or New York, or—gods be thanked—Québec City. And those differences can kill unwary runners.

Differences in customs and laws from area to area are becoming more important as the number of out-of-sprawl runners increases. A noticeable number of street ops have been flowing into the Elliot Bay area from elsewhere on this fine, fragged continent: samurai from Denver and Salt Lake City, riggers from CalFree, shamans from various tribal lands, and hermetics from all over the green earth. Most unusual is a recent influx of deckers from Pueblo; apparently the guys who run the Net down there have gotten a mite twitchy recently, and lots of shadow deckers came here seeking relief from the heat wave.

In any case, it stands to reason that all this new talent—and maybe some of the old talent as well—could use a quick crash course (or refresher, as the case may be) on what's going down in Seattle. I couldn't think of a better way to get the information across than to upload the most recent *Real Life* onto the Shadowland bulletin board system. Of course, I've edited out some hefty chunks of material. What runner (or wannabe) really wants to know about the hot new art gallery throwing a wine-and-cheese opening in Beaux Arts, or where to catch the latest in artsy-fartsy experimental trid? Let the tourists read that drek. You wanna read it, go check out the tourist copy of *Real Life*; this one's got other priorities.

As with everything else on Shadowland, the text itself is read-only; you can't edit it or delete it, but if you really want to try, go to it: we're testing some really hot, new black ice from Pueblo. Also as usual, there's enough free space in storage for as many comments as anyone wants to add. And finally, as always, we take no responsibility for the accuracy of *anything* you berks put up here.]<<<<<
—Captain Chaos, Northwest Neo-Anarchists' League
(18:14:19/1-7-53)

!!SECURITY ALERT!!

RIZE
ONNEL
NLY!

AUTHO
PERSO
ONL

SECURITY BLANKET

Reprinted from Corporate Life, an in-house publication for employees of Mitsuhama Computer Technologies, January 2053

ecurity systems are a fact of corporate life. All corporation employees interact with, and are protected by, elaborate security precautions every day of their working lives.

The high level of security provided by major employers such as MCT constitutes one of the greatest benefits enjoyed by workers: confidence in their safety on the job. Interestingly, though they depend on this safety, many people find the very security precautions that guarantee it highly intrusive and irritating. Simple procedures such as wearing "smart ID" badges, using "slash" cards to open doors, or passing through weapons detectors are looked upon as invasions of privacy, and are circumvented whenever possible.

MCT senior management believes that a brief review of how contemporary security systems operate and the many components of which they consist may serve to demonstrate the need for these systems and encourage all employees to comply fully with all regulations. Describing the great lengths to which MCT goes to protect its employees can only increase the confidence that those employees rightly place in their employer. We hope that by illustrating how the different facets of a security system interact, all employees will recognize that circumventing even the most apparently irrelevant precaution weakens the entire system.

>>>>>[Oh, yes, MCT is *sooo* protective of its employees. It so obviously cares for their individual welfare and their peace of mind...*like drek*. By protecting its employees, MCT protects valuable assets. It costs nuyen to replace a geeked employee, just like it costs nuyen to replace a damaged corporate car. Don't make the mistake of assigning altruistic motives to MCT, or to any large corp.]<<<<<
—Latch (10:43:54/5-8-53)

SECURITY SYSTEM OPTIONS

One of the most important decisions a company must make when designing a security system is whether to follow a centralized or a decentralized paradigm. In essence, the distinction is as follows.

In a *centralized* paradigm, a single, central computer controls the entire system. All security subsystems—from door locks, cardreaders, and retina scanners to alarms, gas dispensers, and gun ports—are designed as peripherals with minimal local "intelligence." Sensors feed mostly unprocessed, raw data to the central computer, which makes decisions based on the data stream. The same computer triggers and/or controls peripherals such as alarms and other active measures. The central computer makes all its decisions based on the information it receives from the peripherals.

>>>>>[A quick aside: "active measures" in the paragraph above *sounds* innocuous, and "gun ports" doesn't sound much more drastic. Don't be fooled, boys and girls. Gun ports and similar "active measures" can ruin the day of the most hardened razorboy. Check out my comments later on.]<<<<<
—Cutter (11:08:10/6-6-53)

In contrast, the individual subsystems comprising the overall system in the *decentralized* paradigm have considerable independent intelligence. In fact, in a true decentralized system, individual subsystems are completely autonomous. Sensors collect data, analyze it, and decide how to respond, all without consulting a central authority. If circumstances warrant, the subsystems trigger an alarm or take other action by sending commands to peripherals connected to them, but not to a central computer system. The designers may decide that autonomous sensors will send update information to a central monitoring computer. Unlike a centralized system, however, in this case communication is unidirectional. The central machine cannot send information or commands to the security subsystems.

>>>>>[Just a quick note from the old Editor: elsewhere in this volume lurks a piece titled **Unidirectional Datalines** that tells all about the kind of one-way communication touched on above. Check it out.]<<<<<
—Captain Chaos (19:21:51/1-7-53)

The following example explains how the different types of security systems may work in practice. A corporate office is protected by a centralized system connected to pressure sensors, maglocks, alarms, door actuators, and gas dispensers. When an intruder enters the office building and tries to break into a restricted area, he or she treads on a pressure sensor, which sends a digital signal to the central computer. Because this may be an anomalous reading, the computer triggers only an internal alert, not a full alert, and increases the sensitivity of other sensors in the area. Seconds later, the intruder tries to defeat a maglock. The maglock sends a "tamper" signal to the central computer. Together with the pressure-sensor signal, the computer has now received enough cues to trigger a full alert. It sounds an audible alarm, closes all doors in the area, freezes all maglocks, and floods the area with gas. It is important to understand that the same central security computer will be monitoring and controlling other peripherals throughout the building.

In a decentralized system, the pressure sensor connects to the maglock, the door actuators, an audible alarm, and the gas subsystem, but not to a central computer. Though the same process takes place when the intruder trips the pressure sensor and then tampers with the maglock, the decisions are made entirely within the subsystem monitoring that area of the building. The overall result is the same: doors shut and lock, the alarm sounds, and the gas is released. If the designers built a report structure into the system, the subsystem establishes a connection to a central monitoring computer and reports an alarm condition. Note that only the subsystem can establish such a connection; the monitoring computer cannot request a report.

A centralized paradigm offers many advantages. The first lies in cost savings. The central control computer must have significant processing "horsepower," and thus will be very expensive, but the individual peripheral units are "dumb"—i.e., they have little or no local processing power—and so cost much less. For example, a pressure sensor can consist of a simple on-off switch with a few wires attached. Ease of control provides another major advantage. A single operative stationed at the central computer can monitor and control the entire security system. It is also easy to upgrade or alter system responses by simply reprogramming the single central computer. And finally, centralized systems minimize the potential for false alarms. Because all subsystems communicate continuously with the central computer, the central system can compare data streams from multiple sensors and decide, using probabilities, if a given sensor is faulty.

Decentralized systems, for obvious reasons, cost much more. Each peripheral or subsystem must contain processors capable of analyzing data and making decisions. Upgrading the system, or altering response options, requires reprogramming each processor. Because these processors are not interconnected, reprogramming becomes a time-consuming process. Also, a fault in a single sensor could theoretically trigger a full-fledged alarm response in an area not requiring such a response.

The major disadvantage of a centralized security system is that the central computer represents a security risk. Because the central computer controls the entire security system, he who controls the central computer controls the system. By penetrating that single computer, a decker gains absolute power over every security subsystem connected to it. This decker can open locks, silence alarms, deactivate sensors, and generally manipulate the whole system as he pleases.

>>>>>[Yahoo, that's me! Actually, it's not as easy as this article makes it sound. Security computers usually pack real nasty ice designed to ruin the day of any decker who tries to tangle with it.]<<<<<
—Bit Basher (12:54:55/8-11-53)

>>>>>[But that's what makes it fun...]<<<<<
—Shane (01:47:01/8-17-53)

A centralized computer system can be further compromised if the computer controlling the system is connected to the Matrix or uses bidirectional communication with any system connected to the Matrix. This kind of connection allows any decker with access to the Matrix to penetrate and disable the entire security system.

>>>>>[Sounds real dumb, doesn't it? Who'd do something like that, you ask? Lots of people. Small companies frequently try to shave costs by getting their central computer system to run everything: accounting, telecommunications, building maintenance, and security, avoiding the cost of buying a second oh-so-expensive computer just to run the maglocks.

But what does that mean? It means that the same computer hooked into the LTG to take care of customer service provides Matrix access to the security system…which means that you or I can come prancing down a dataline and have our nefarious way with that company's security. Believe me, jokers, plenty of companies out there handle things this way.]<<<<<
—Latch (10:51:29/5-8-53)

>>>>>[Yeah, but anybody bush-league enough to handle things that way won't have anything worth taking.]<<<<<
—Chipper (19:32:00/10-23-53)

Isolating the centralized security computer from the Matrix and from all other computers within the corporation achieves a slightly enhanced level of security. The risk of decker penetration is still very real, but is diminished considerably.

>>>>>[This system forces the decker to *physically* penetrate the corporate site before jacking in. That is, he or she has to move his or her precious meat body into the facility, find some form of electronic access to the central computer, and *then* rape the hell out of it. Barbaric.]<<<<<
—Pzip (00:03:50/4-29-53)

>>>>>[Barbaric maybe, but better than nothing. With the right kind of hardware, you can jack into any sensor or actuator connected to the system. In other words, make a hardware connection between your deck and the guts of a maglock, and you're in.]<<<<<
—Latch (10:55:06/5-8-53)

>>>>>[This kind of paradigm—let's call it "isolated centralized"—is the most common set-up in the sprawl. Only the really big boys, with lots of nuyen to throw around, go the fully decentralized route for every system. Most smaller corps save decentralized systems only for the *most* sensitive, restricted stuff…which is, unfortunately, what most of us want.]<<<<<
—Neon (23:31:21/7-7-53)

SENSORS AND DETECTORS
This section describes some of the most common sensors used in corporate security systems. (In this context, "sensor" refers to any system that can detect and/or identify intruders, or distinguish between authorized and unauthorized personnel.) Most of these are in use somewhere on MCT property.

Ident Systems
An ident system requires a subject to offer proof of and then confirms his identity before allowing him to proceed into an area. Ident systems usually connect directly to maglocks or door actuators, so that a door will open only for personnel authorized to pass through it.

An extensive array of different ident system technologies exists, some of them dating back to the middle of the previous century. Several of the more common systems are described below.

Keypads
Personnel must enter an identification (ID) code that serves as a password on a numeric or alphanumeric keypad. Anyone unable to provide a valid code may not pass. The ID code also logs the subject's identity and the time he or she passed through that particular security point.
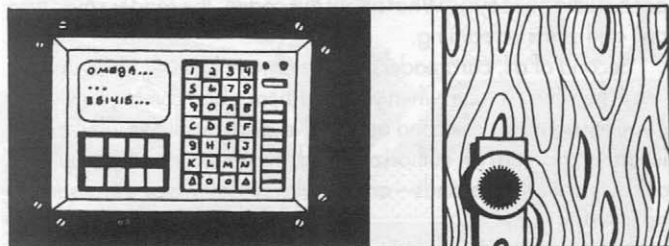
>>>>>[Obviously, to beat this kind of system, just extract the appropriate code from an authorized employee, either by cunning or straight interrogation/intimidation. A keypad box can't recognize the person punching in the code, and won't care as long as the code is valid.]<<<<<
—Pzip (13:13:39/8-8-53)

>>>>>[…which is why any security system worthy of the name backs up the keypad with something else, like video cameras.]<<<<<
—Torrence (20:50:01/9-22-53)

>>>>>[If you can't get a valid code by hook or by crook, start jiggering the system. Theoretically, you can take the faceplate off the keypad and muck with its circuitry until it lets you in. Unfortunately, many keypads now have anti-tamper circuitry that triggers an alarm if the faceplate is removed, or are simply armored so you can't take the faceplate off with anything less than an anti-tank weapon (which would also trigger an alarm).]<<<<<
—Slider (03:45:18/9-26-53)

Cardreaders
Two main types of cardreader currently enjoy popular use: the "insert-remove" style, and the so-called "slash" system in which the edge of the card is dragged through a slot. Both work by reading an identification number encoded on the card, either "written" on a magnetic strip or stored in a tiny microchip within the card.

>>>>>[Again, the easiest thing to do is get a valid card. You just steal the damn thing—but use it before someone misses it and reprograms the system, making the code on your new possession useless.]<<<<<
—Pzip (13:21:11/8-8-53)

>>>>>[I've run into some real snake oil salesmen on the streets peddling boxes they claim will defeat cardreaders. They usually give you a deal—about 5,000¥. Supposedly, they work just like the ones you see on the trid adventure shows: plug a fake card into the cardreader slot, and the little black box runs through all the possible permutations and combinations until it hits the code that satisfies the cardreader.

Unfortunately, what you see on the trideo doesn't work in real life. (Big surprise, right?) First off, many cardreaders are programmed to trigger an alarm the first time they read an invalid code. (This happens a lot in highly sensitive environments.) So the first time your hot little box says, "What about *this* code?" the reader says "frag you" and starts screaming.

Second of all, cardreaders almost always have a pause built in. Even if they don't scream when you feed them a bad combo, they won't let you try again for a second or two. (Keypads work this way, too.) If the reader misreads an authorized card, the employee simply pulls his card out, waits two seconds—one one thousand, two one thousand—and inserts it again.

Now consider the black box that tries all the possible codes until it hits the right one. No matter how fast the electronics in the box, each try takes *at least* one second—the time-out period programmed into the reader. That makes the box totally useless. Let's say the code has only 5 numeric digits: that gives you 100,000 possible codes. Trying them all would take 100,000 seconds, or 1,667 minutes, or about 28 hours. And that's for a ludicrously simple code. An average card system code runs ten characters or more, alphanumeric, which gives you 36 to the 10th power—36^{10}—or more possible codes. Running those would take your wiz little box just a little more than one hundred million years.]<<<<<
     —Buzz (14:27:46/10-23-53)

>>>>>[Some devices will do the job, but they work on different principles. And, predictably, they cost a *lot* more: 10,000¥ and up!]<<<<<
     —Luke (08:11:09/10-30-53)

>>>>>[You slags know the easiest way to bust into any system? Go have a long, hard talk with the guys who programmed it. Any programmer worth his salt leaves some kind of back door into the system, some way he can get in to make repairs if the system goes down. Just get him to tell you how to find the back door and how to open it.]<<<<<
     —Barnes (13:03:10/7-9-53)

>>>>>[Barnes has a point, though he makes it sound easier than it is. For one thing, just tracking down the programmer might be a big job. He may not even be around to help. Plenty of urban folk tales talk about major corps that get a drek-hot programmer to whomp up a good security system, then mindwipe him, put a thought-lock on his memory, or just clean flatline him.

If the programmer's still around, the back door might not be. Once it installs a system, bet your assets a corp will send its deckers romping and stomping through the code to close every back door they can find...or maybe just boobytrap them nine ways to Sunday.

Bottom line is that trying to take out a system through the back door is *not* the end of your problems—it's often just the beginning.]<<<<<
     —The Finn (09:11:51/8-30-53)

Print Scanners

The most common print scanners digitize and analyze thumb- or fingerprints, palmprints, or retina scans, respectively representing higher levels of security. Modern technology makes the scan-analyze-recognize cycle very fast, often less than a second per entrance request. Even though print scanners efficiently balance convenience and reliability, these systems are sometimes inappropriate because they require the employee to remove hand or face protection.
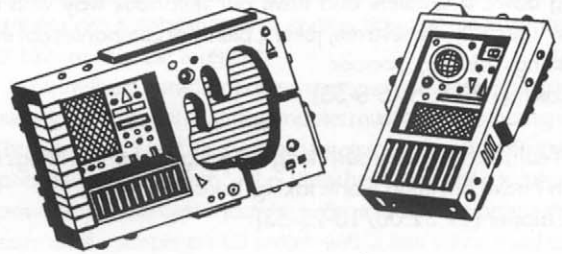
>>>>>[False fingerprints and false palmprints have been around since the last century, usually taking the form of thin, sometimes monomolecular, plastic membranes covering the finger or palm and bearing an alternate print pattern. People have improved the technique, of course, and it'll spoof bargain-basement print scanners. But the top-of-the-line scanners have secondary circuitry that checks for authenticity using chemical sniffers, galvanic skin response meters, and so on to make sure it really *is* skin they're reading.]<<<<<
     —Cap'n Zapz (15:12:17/9-11-53)

>>>>>[The name of *that* tune is that the print scanner is happiest when it's really reading the finger, thumb or palm it expects. Of course, the willing participation, or even presence, of the owner of said extremity is a technicality, if you get my drift.]<<<<<
     —Cain (21:13:40/10-5-53)

>>>>>[I get your drift, you butcher, but it might not help you. A sophisticated scanner will pass a low-voltage charge through the extremity and measure the conductance—which varies wildly between a severed thumb and a thumb attached to a living body. It will probably check temperature and other things as well.]<<<<<
     —Pauley (00:45:19/10-24-53)

>>>>>[Surgically implanted false retinal patterns *can* fool a retinal scan, but not reliably. And because possessing or implanting a false retinal pattern is a capital crime in the UCAS and most other countries, lack of reliability becomes an issue. If you want to pay the nuyen, you can get a modification more likely to fool the scanners, but it costs. Also, the more detailed the replication, the more invasive the work. Think twice about this kind of thing.]<<<<<
     —Buzz (14:33:44/10-27-53)

>>>>>[Hey, can anybody out there enlighten me on one small point? I paid a little visit to the Gaeatronics research facility up near Port Gamble and saw something really weird. Retinal scanners and what looked like thumbprint scanners all over the fragging place...but all at knee or waist height. Why?]<<<<<
     —Color Me Curious (15:31:23/5-1-53)

>>>>>[I've heard rumors about this, but I don't know if I should believe them. According to the buzz I picked up, Gaeatronics uses shapeshifters to guard the place, and those scanners you saw were for retinal patterns and *nose prints* of intelligent animals!]<<<<<
—Atkins (19:33:33/6-15-53)

Voice Recognition

Voice recognition remains one of the least intrusive and most effective security systems. The voice subsystem contains a digital "voice model" for each authorized person. To open the door or disarm the alarm to which the voice system is connected, the employee simply speaks a short phrase containing a representative sampling of phonemes. If the subject's voice matches a valid voice model, within the parameters of normal error, the system accepts that person as authorized.

>>>>>[Yeah, and if the poor sap's got a cold, or a frog in his throat, it calls the Gestapo.]<<<<<
—Baylock (23:14:55/4-10-53)

>>>>>[Urban folk tale. They licked that problem last century. Remember, every voice has secondary harmonics, resonances, and other characteristics that *don't* get slotted up when you get a cold. Only serious trauma to the larynx, like a hard punch to the throat, can change the voice enough to screw up the system.]<<<<<
—The Finn (19:28:58/6-30-53)

>>>>>[How do you crack this one? Make it worth an authorized person's while to speak the right code—like, offer him lots of money, or the chance to continue breathing. Or you can record the guy's voice when he speaks the phrase, then play it back.]<<<<<
—Del (14:30:59/7-20-53)

>>>>>[Right on one, Del, wrong big time on the other. Most recording techniques add some kind of distortion to the sound, however slight, that good voice recognition systems can detect. Yes, even digital recordings: if the sampling rate, or quantization rate, on the recording does not exactly match the sampling rate of the recognition unit, you're blown. (And you can bet that major corps pay the nuyen for the best.)

On the topic of tech and nuyen, how many people out there have paid the 95,000¥ for a voice modulator with a secondary pattern, or one of those god-awful Wiremaster internal voice-mask things, hoping to get past voice systems? Well, dream on, jokers. Unless you pay *really* big nuyen, you won't fool any of the good subsystems.]<<<<<
—Buzz (14:39:40/10-23-53)

>>>>>[Hey, wait a tick: this Real Life drek is supposed to be a kind of snapshot of what Seattle's thinking about this week, right? What does it say about Seattlites, that the lead article talks about security systems, hmm?]<<<<<
—Bung (14:16:08/10-5-53)

>>>>>[Paranoid city.]<<<<<
—Brain Buffer (09:06:17/10-10-53)

VOICE PRIN'
NEGATIVE·N

DAN(

DAPH

>>>>>[Do you blame them? Look at the number of social deviants logging on here to post suggestions on how to crack security systems, including gems like "cut the guy's thumb off." Just because you're paranoid doesn't mean everybody *isn't* out to get you, cobber.]<<<<<
—Sheaffer (23:08:51/10-21-53)

>>>>>[By the way, chummers, I hear some really sophisticated recognition systems are just starting to hit the streets that incorporate sophisticated vocal stress analysis algorithms. (Read "lie detectors.")]<<<<<
—Fang Face (14:15:41/10-22-53)

Door and Window Alarms

The technology used in "perimeter" subsystems, such as those securing exterior doors and windows, has changed little since the middle of the 20th century. Under the principle of "if it isn't broken, don't fix it," the technology stays the same because it remains effective.

Door Alarms

The door alarm is by far the simplest warning system in use today. Electrical contacts installed in the edge of the door and in the door frame make contact when the door is shut, creating a closed electrical circuit. Opening the door so that the contacts no longer touch breaks the circuit and triggers an alarm.

>>>>>[Surprisingly tough to get around this one. Bypassing the system involves a basic principle: just make sure that the circuit remains complete and unbroken. Looks easy: attach one end of a wire to the contact on the door and the other end to the contact on the frame, then open the door. The wire maintains the closed circuit. The trick, of course, is *getting to* the contacts. When the door's closed, the contacts are pressed against each other and usually protected by a metal flange. You might try digging into the door and frame material, but macroplast or cold-rolled steel makes that difficult. Even if you reach the contacts, the wire trick may not work. Really paranoid designers will have installed circuitry to detect the change in resistance when the current runs through the wire.]<<<<<
—Slider (04:10:38/9-26-53)

>>>>>[Frag opening the door—just go *through* it. Or go through the wall next to it, if the conditions are right.]<<<<<
—Hammerman (18:00:53/11-8-53)

>>>>>[Forget the alarms on the door. Concentrate on convincing the rest of the system that the person coming through the door is authorized.]<<<<<
—Pzip (20:11:08/12-5-53)

Window Alarms

Windows that open use the same security technology as doors: contacts on the windows and the frame complete an electrical circuit when the window is closed. To prevent an intruder from simply smashing a glass window and gaining entry, most security system engineers apply a thin metallic foil strip around the periphery of the window glass and run a small current through it. Breaking the window snaps the foil, breaking the circuit and triggering an alarm.

>>>>>[Use a glass cutter to make a hole in the center of the window.]<<<<<
—Chipper (08:18:41/4-12-53)

>>>>>[…But be *real* careful when you crack the glass out of the hole you cut. The system engineers often build a dedicated-duty sound detector into the window frame, which sounds an alarm in response to the specific set of transients and harmonics associated with cracking glass.
Now, all this applies only if the architect put glass in the window. Glass is getting rarer and rarer. Various forms of polymers, transparent construction plastic, and so on seems to be the way to go now. Most will resist impacts, even from a hammer or a bullet, and they're a cast-iron bitch to cut. Some conduct electricity, allowing the security designers to pass a low current through the whole window. With those materials, if you *do* manage to cut a hole in the center of the pane, you've changed the mass—and thus the conductance—of the plastic sheet. The current fluctuates, and it's alarm city.]<<<<<
—Slider (04:12:49/9-26-53)

Cameras

Another tried and true, simple but effective security system is the closed-circuit video camera, still in wide use. Scanning or fixed-view cameras watch sensitive areas, running the video feed back to display screens in a secured control post, where guards keep a constant watch for anything out of the ordinary. In recent years, expert system and primitive artificial intelligence (AI) software has given computers a limited capacity to "observe" the video feed themselves and "notice" unusual events or presences. In most cases, the limited decision-making capabilities of these systems do not allow them to make an autonomous response. Instead, the computer alerts a (meta)human security guard to the anomaly it has spotted, allowing her or him to decide how to proceed.

>>>>>[I've seen some autonomous decision-making from test computer systems that would curl your hair. On a conservative estimate, I'd say we've got three to five years before all those fat-dumb-and-happy security guards sitting at banks of monitors move over for computer systems that never fall asleep, never go to the can, never go out for donuts, and never miss *anything*. Scary.]<<<<<
—FastJack (18:28:11/2-27-53)

>>>>>[Until then, fooling a camera system actually just comes down to fooling the guy who's watching the screen, thank god.]<<<<<
—Buzz (05:18:31/3-1-53)

>>>>>[Cameras are easy to handle. Just turn out the lights. Simple.]<<<<<
—Mack (19:06:08/3-15-53)

>>>>>[*You're* simple, Mack. Dontcha think the security guards will notice, and take steps, if the lights "coincidentally" go out in a sensitive area?]<<<<<
—Chrome Cat (18:20:36/3-17-53)

>>>>>[Just take the time to arrange things so the guards think everything's kosher. Make the lights-out part of, say, an authorized repair crew testing the circuits.]<<<<<
—Chipper (08:38:45/4-12-53)

>>>>>[Most camera systems these days use low-light to see just as well in IR as visible light. Makes the whole argument academic, neh?]<<<<<
—Slider (04:20:58/9-26-53)

>>>>>[You want the easiest solution, call in your friendly neighborhood decker. Get him to crash into the control system and frag it to feed a false signal to the monitor. It doesn't matter *what* the camera sees; only what shows up on the guard's monitor matters. Set up a loop a minute or so long of the data stream the camera was sending when the hallway (or whatever) was clear. Then no matter what happens in front of the camera, the monitor shows empty hallway.]<<<<<
—Pzip (20:13:52/12-5-53)

Lasers

Corporate facilities often use lasers to secure sensitive areas during non-working hours. Contrary to what often appears on the trideo, these lasers never produce a concentrated enough beam to inflict damage on an intruder. They simply function as sensitive intrusion-detection devices. In most systems, half-silvered mirrors split the beam from a single laser emitter into multiple paths. An array of small mirrors reflects these beams many times so that the beams crisscross the restricted area. The path of each beam ends in an optical detector. If an intruder passing through the area breaks the beam, the detector senses the interruption and triggers an alarm.

Though some corporate environments still use visible-light lasers, most security systems now use infrared lasers that emit beams invisible to (meta)human eyes.

>>>>>[Visible-light lasers are just as tough to spot as IR lasers if the air's free of dust and other gunk. In clear air, you simply can't see the beam.

I know some of you smug-as-drek jokers out there dismiss the danger of IR lasers while thinking lovingly about your IR-sensitive cybereyes or goggles. Well, don't get complacent. In a dust-free environment, there's nothing to scatter the IR light, either, so even your chipped-up optics won't see the beam until you put your eye right in the light path. And that, of course, sounds the alarm.]<<<<<
—Buzz (15:00:19/10-23-53)

>>>>>[So produce your own dust. Smoke works okay, but aerosols work better. Even hairspray does the job.]<<<<<
—Chrome Cat (12:03:46/11-10-53)

>>>>>[In some cases, yes. But if the system designer tried to cover all the angles, he or she will have set the optical detector sensitivity so high that it'll detect even the tiny decrease in beam intensity caused by your smoke or aerosol spray. I'm not kidding. I almost got burned by a system like this once.]<<<<<
—Buzz (05:12:18/11-14-53)

>>>>>[Even if you *can* somehow detect the beams, seeing them might not help you. Any halfway competent designer splits and bounces the beam until it forms an interlocking meshwork of lasers acrobatically impossible for *anyone* to snake his way through.]<<<<<
—Pasternak (13:22:08/11-16-53)

>>>>>[I've had the unique honor of seeing a guy called Wraith work a laser security system. On two separate occasions I saw him defeat infrared lasers, the first time re-diverting the beam paths with his own array of mirrors and the second using a fiber optic light pipe to literally *bend* the beam out of the way. He was sheer poetry in motion.]<<<<<
—Lang (23:11:51/12-13-53)

>>>>>[You use the past tense, Lang. Does that mean what I think it means?]<<<<<
—Buzz (23:25:11/12-15-53)

>>>>>[I describe Wraith's death from a run-in with monowire strung across a doorway further on in this file. A nasty way to die.]<<<<<
—Lang (08:13:27/12-20-53)

>>>>>[You know, Wraith got fragging lucky on the two occasions you described, Lang. In a good laser system, the drop in beam intensity caused by changing the beam path with mirrors or running it through a light pipe would trigger the alarm.]<<<<<
—Buzz (00:36:01/12-23-53)

>>>>>[Wraith *wasn't* lucky, he was *good*. In the first case, his calculations included adjustments to keep the length of the beam path unchanged. In the second, he had researched the system and knew the subsystem didn't include an intensity trigger. Wraith left *nothing* to luck.]<<<<<
—Lang (20:13:30/12-27-53)

>>>>>[Do I detect a touch of hero-worship, Lang?]<<<<<
—Bung (12:13:31/12-29-53)

>>>>>[If so, it's understandable. Lang is Wraith's younger brother, so back off.]<<<<<
—FastJack (00:30:30/1-2-53)

>>>>>[Predictably for an MCT house organ, this piece conceals an unpleasant fact. *Some* laser systems pack enough joules to inflict *very* serious damage on an intruder. A high-enough yield laser will be easier to detect because it partially ionizes the air, something for you runners to look out for. Lethal systems, like several in use at MCT, operate on a two-step process. Normally, the laser emitter produces a low-energy infrared beam as discussed above. But when the beam is broken, instead of sounding an alarm—or *as well as* sounding an alarm—the emitter pumps out a short pulse of high amplitude laser light. (I'm talking *VERY* high power here. The laser's attached to a couple of massive capacitors that have been charging for hours.) The response takes microseconds, and so the part of the intruder's anatomy that broke the low-intensity IR beam gets blasted off with an energy pulse more powerful than a shot from a military-grade laser weapon.]<<<<<
—Roger (11:11:41/1-4-53)

Pressure Detectors

Despite its ultimate simplicity, a pressure detector installed beneath carpet or other flooring may be one of the most effective intrusion detection systems available. Though virtually unlimited in size, cost issues usually restrict pressure pads to less than 15 square meters. Because they operate on a passive principle, and often consist solely of non-metallic components (for example, conductive polymer-resin), they are difficult to detect. Pressure detectors make an ideal complement to biological security (guard animals) because the detectors can be calibrated to ignore objects of the animal's weight.

>>>>>[That 15-square-meter limit isn't much of a limitation when you get right down to it. The average corridor measures two meters or less across, and so a wall-to-wall pad can be 7.5 meters long, or almost 25 feet. Assuming the designer has set things up right, any touch on the pad sets off an alarm. That means you've got to clear the pad. Can *you* long-jump 25 feet? Silently? Carrying the kind of gear most runners pack?]<<<<<
—Chrome Cat (14:14:53/4-5-53)

>>>>>[That question is academic if you don't know the pad's there, wouldn't you say?]<<<<<
—Pzip (22:11:15/5-10-53)

>>>>>[Any company that claims to calibrate the pad to ignore guard doggies is just trying to mislead the public. Depending on whether it's strolling or sprinting, a cyber-equipped attack rottweiler will apply very different pressure to a pad. In general, if a company uses biologicals, they won't use pressure detectors.]<<<<<
—Latch (17:12:41/6-11-53)

Vibration and Air Pressure Detectors

Generally constructed using a magnetic diaphragm within a charged solenoid, vibration detectors sense the faintest of vibrations in the air or floor. Sophisticated computer software analyzes the waveforms of detected vibrations and distinguishes between naturally occurring disturbances, such as seismic microevents or the natural swaying of a building in a high wind, and those characteristic of an intruder.

Air pressure detectors, as the name implies, use a diaphragm to detect changes in air pressure within a room, particularly those caused by a door opening or closing, or someone or something moving within the monitored area. The software analyzes the change and then distinguishes between an actual intrusion and normal changes in barometric pressure.

>>>>>[Note the comment about the system detecting the "natural swaying of a building in a high wind." How much does your standard ferroconcrete-and-construction-composite skyraker sway when a gust of wind hits it? Not fragging much, is the answer. 'Nuff said on how sensitive these things get.]<<<<<
—Pug (02:07:08/2-12-53)

>>>>>[The only way to defeat these sensors is to move *real* slow and *real* quiet, and hope the detector thinks you're a natural air current or a low-flying SST or something. In other words, good fragging luck!]<<<<<
—Chrome Cat (23:14:45/3-15-53)

>>>>>[Remember, you're not trying to fool the detector in this situation: it will "hear" you no matter what you do. You want to fool the analysis software that decides whether a waveform is a breeze or a bogie. As any decker can tell you, waveform analysis software ranges in effectiveness from useless to almost omniscient.]<<<<<
—Bit Basher (13:06:59/8-11-53)

>>>>>[I've heard rumors of portable rigs that produce vibrations exactly out of phase with any sounds a person makes, canceling those sounds out and making him completely and utterly silent, essentially "invisible."

Like I said, though, I've only *heard* about these things. I've never seen one, and I've never talked to anyone who's seen one. Can anybody out there enlighten me? Do these things actually exist?]<<<<<
—Hope (12:39:44/10-12-53)

>>>>>[Dream on, Hope. Theoretically, it's feasible—*just*—but the practicalities make it impossible. For one thing, to cancel out all sound, you need to know the exact distance and bearing from the source of the sound (like your foot scuffing the floor) to the detector. Unlikely you'd have that information. And the realtime processing requirements are just rude. You'd need an MSX-Cray supercomputer to do the number-crunching, and those huge things don't fit in a backpack.]<<<<<
—Mr. Miracle (22:42:50/12-21-53)

>>>>>[A nasty variation on this theme is the heartbeat detector, an ultra-sensitive microphone attached to a spectrum analyzer specifically designed to detect the sound of a beating heart. The setup costs a bundle, running in the 20K¥ range, I'd say, but it's almost impossible to defeat. Because the sound of your pulse is conducted to every part of your body, you can't possibly mask it. If you come up against something like this, you're almost certainly hosed.]<<<<<
—Pzip (02:10:09/12-22-53)

>>>>>[Air pressure detectors are another bear. They're usually set up in a room so that opening the door—even going *through* the door or the wall—changes the ambient pressure of the room and triggers an alarm. I thought of one, complex way to get around this system: set up an "airlock" around the door, maybe using some kind of light, flexible plastic sheeting. Step into the airlock, and pressurize it (or *depressurize* it) to match the pressure on the other side of the door. The pressure difference will probably only be measurable in hundredths of kilopascals (kPa), or thousandths of a pound per square inch (psi). (Measuring the air pressure on the other side of the door with sufficient accuracy is the rub…) Anyway, once the two pressures equalize, you should be able to open the door without setting off an alarm. Of course, you've *still* got to sneak across said room without creating any air currents.

I know, I know, too complex, too many things to go wrong. But I really can't think of any better way to defeat this one.]<<<<<
—Straight Gain (15:51:08/12-22-53)

>>>>>[You mundanes would make me laugh if you weren't so pathetic. You always look for the technological answer to every problem. Vibration detectors? Heartbeat detectors? A simple spell of silence is all it takes.]<<<<<
—Trevor (14:52:10/12-24-53)

>>>>>[Um, yeah...]<<<<<
—Shrimp (23:52:41/12-24-53)

ACTIVE RESPONSE MEASURES

The subsystems discussed above represent a few examples of the technology available to detect intruders. Detection is only part of the security equation, however. Once detected, intruders must be contained or neutralized, the task of active response subsystems.

The simplest active response measures are alarms: audible, visible, silent, localized, or general, the type used determined by the circumstances. Depending on whether it seems expedient to inform the intruders that they have been detected—which knowledge alone sometimes prompts the intruders to leave of their own accord—alarms range from the flashing lights and wailing sirens familiar to trideo and simsense aficionados to a simple neural cue given to a single guard jacked into the security desk.

Containment Responses

The most common response to an alarm is to channel, immobilize, or otherwise constrain intruders. One popular containment method resets or freezes all maglocks in the affected area. The reset or frozen locks can be opened using a specific code or a card possessed only by security personnel. Thus, intruders who penetrated the facility using a stolen or copied card cannot leave the area using the same card. In a centralized security system, the alarm response may shut down *all* locks in the area, requiring a specific action order issued by the central monitoring computer to open each lock.

High-security installations often use mechanical doors to seal and compartmentalize the area in which an alarm sounded. Though horizontal sliding doors actuated by servo motors remain the most common choice, maximum-security systems use vertical sliding doors. Designed to withstand any assault from inside or out, a single door is usually constructed of a half-meter-thick slab of homogenous steel, weighing approximately 20,000 kilograms (22 imperial tons), that falls under its own weight upon the release of a restraining latch. The resulting barrier proves almost impregnable, because the door is too thick to cut through quickly, and too heavy to lift. The system cannot be circumvented, as the motor used to winch the door back into its "ready" position requires a special security identification code to start up. Vertical sliding doors usually close if electrical power is cut.

>>>>>[These vertical doors really are as tough as they're advertised. A chummer of mine says they use this system in the Renraku arcology to protect particularly sensitive areas. I reckon your standard cutting torch would take maybe an hour or so to penetrate half a meter of homogenous steel—and that's to drill a hole the diameter of your torch flame (or laser beam, if you've got power packs beefy enough to keep a laser burning for an hour), *not* to cut a hole big enough to be useful.]<<<<<
—Pzip (16:29:22/4-10-53)

Neutralization Responses

The security industry has developed several methods of neutralizing intruders once detected and constrained. The simplest method floods the area in question with one of several available knockout gases, of which Neuro-stun VIII is the most effective.

>>>>>[Pretty predictable that this rag pushes Neuro-stun, since MCT holds the manufacturing license for it—indirectly, of course. Also predictably, they gloss over the fact that a lot of corps use nastier stuff than knockout gas. The way I understand it, a couple of corps in the plex use Green Ring 3, and some even spray Seven-7—both gases developed for use in war and offering unsurpassed lethality (and immense illegality, as if it matters). You were warned.]<<<<<
—Hangfire (14:11:37/2-14-53)

Another popular neutralizing option sets the alarm to trigger a gun port in the invaded area. This response cannot be used in areas containing breakable objects, of course. At the discretion of the company, the gun ports may fire rubber bullets or mild tranquilizing darts, each temporarily disabling the intruder for easy apprehension by corporate security.

>>>>>[Tell me about gun ports, you say. Okay, I reply, but don't say I didn't warn you. A gun port consists of a box built into a wall or the ceiling containing nothing but the mechanism of a very nasty autofire weapon, a little servo motor, and a *whole lot* of belt-fed ammo. When something or someone triggers the alarm, the box pops open and the gun hoses down the area until it runs out of ammo. Nothing fancy about this system: no aiming, no sensors. The servo plays the gun around to "suppress the area." I've seen gun ports built around old-style M16 assault rifles, more modern assault rifles, and—for those who care enough to send the very best—fragging Vindicator miniguns. Ammo load usually numbers in the hundreds of rounds...just to be sure.

How do you defeat a gun port? *Don't trigger it.* That's it. Once you trigger it, you're meat, unless you're good at dodging minigun fire. Naturally, the corps set up these things in areas lacking viable cover. Sometimes the designers install more than one in order to set up crossfire.]<<<<<
—Blacque Jacque (03:16:52/11-11-53)

>>>>>[Rumor has it that some outfits are experimenting with "intelligent" gun ports. The security boys hook the guns up to sensors (cameras, IR detectors, motion detectors, and so on) and a computer with pattern recognition capabilities. When intruders trigger an alarm, the gun pops out, but targets and fires only at those things the computer recognizes as an intruder. These experimental systems cost plenty. For a system used to kill intruders, a standard "dumb" gun port is much cheaper, so we can assume that the people playing around with the intelligent models will equip them with Narcoject weapons.

I don't know from experience, but I'd guess the "smart" ones are easier to beat. Simply blind the sensors (if you can find them), and the thing's useless. You might also be able to fool the pattern-recognition processor. To repeat an earlier comment: you don't need to fool the sensors, you need to fool the software.]<<<<<
—The Hammer (16:58:20/12-29-53)

CONCLUSION

Even the minimal information provided by this overview reveals the extent and complexity of corporate security. The systems themselves are complex, interconnected mazes of pitfalls and traps set for the unwary and unauthorized, unmapped territory that should make obvious the need for all employees to comply with security regulations for their own safety and the safety of their families and coworkers. Individuals interested in pursuing the topic further may contact the corporate library.

>>>>>[MCT naturally chooses not to discuss the more experimental nasties currently in development, the first of which includes EMP units designed to hit an area with a strong enough electromagnetic pulse to really frag with electronics...*including* things like the motor actuators of cyberware and the physical interface between headware and your nervous system. EMP takes a hell of a lot of power, so it's very expensive. But it also works damned well.]<<<<<
—Knightshade (07:15:13/3-16-53)

>>>>>[Companies interested in non-lethal takedowns are getting creative. Buzz on the street says Aztechnology has installed "dart bombs" in some corridors. Something like low-power frag grenades, dart bombs spray low-velocity, flechette-like darts tipped with Narcoject instead of shrapnel. Impact armor blocks the darts, but if you're close to the bomb when it goes off, you'll look like a pincushion and probably take one or more darts in any patch of exposed skin.

An even wilder rumor about some weird layered defenses came my way recently. Starting with dart bombs to take out unarmored intruders, these defenses follow the darts with contact sleep gas to take out people without chemsuits, then add radiant heat to make it so hot that anybody who doesn't take off his chemsuit and armor keels over from heat prostration. Another round of dart bombs and sleepy gas finishes off stragglers.]<<<<<
—Barlow (09:57:26/3-22-53)

>>>>>[Seems like a lot of trouble and expense. Why don't they just use *real* frag grenades and get it over with?]<<<<<
—Tex (11:18:58/4-1-53)

>>>>>[Dead men tell no tales, but live ones can be downright talkative. (I read that somewhere.) As a point of fact, a live prisoner can always be made dead, but the reverse poses a few problems.]<<<<<
—Doc (17:59:23/4-4-53)

>>>>>[Some corporations use monowire to protect sensitive areas. They stretch one or more strands of the stuff across a doorway or hall, and anybody who walks into the wire gets sliced apart. A colleague of mine died this way when he walked right into a monowire strand at knee-height. It sliced both his legs off. He died quickly, but not pleasantly.]<<<<<
—Lang (10:22:19/6-23-53)

>>>>>[*Very* nasty. Even under perfect lighting conditions, monowire is damn near invisible.]<<<<<
—Street Trash (23:57:10/7-11-53)

>>>>>[And here's another charming thought.

You know that every crystal has a characteristic resonant frequency, right? And that high-amplitude sound at that frequency will shatter the crystal? (Like an opera singer shattering glass with her screech.)

You also know that optical chips, both memory and processor, are based on crystals, just like laser sights and lots of other wizzer tech, and that everybody and their dog buys crystals to use in their own products from the few crystal manufacturers in the world. And, finally, each manufacturer generally makes only a dozen or so different crystals.

Can you see where I'm leading? (I can hear the "uh-ohs.")

I figure that all the tech you own has fewer than 100 different formulations and sizes of crystal. Each of those crystals has a different resonant frequency at which it will shatter. That means a security system can flood an area with high-amplitude sound, cycling through only about 100 distinct frequencies, and shatter *every drek-fragging crystal in everything you're carrying*, including laser sights, rangefinders, comm units, maybe even the crystals in your headware.]<<<<<
—Wintergreen (12:10:42/9-28-53)

>>>>>[Doesn't even bear thinking about.]<<<<<
—Chrome Cat (15:43:11/10-1-53)

>>>>>[Somebody said it earlier, but I'm going to say it again. Why fool around with all this tech trash? Send in a mage or a shaman. Invisibility and silence spells defeat cameras, lasers, and sound/air pressure detectors. Levitation takes the mage over any pressure pads on the floor. Use telekinetic skills where appropriate. Lay control thoughts and influence spells on any guards who happen to wander past.

In some situations, the mage need not even enter the area physically. Travel astrally, and no electronic detector in the world will sense your presence. Simple.]<<<<<
—Gandalf II (10:41:10/10-28-53)

>>>>>[You're the only simple thing here, Gandalf. If you have enough magical talent to do what you describe, you can also assume that your opponents—the people protecting the area you want to penetrate—have as much talent, or more. As many ways exist to block an intruding mage as ways for the mage to frag with the security systems—maybe more. Just off the top of my head I can give you a good list of unpleasantness to expect. Magical barriers, for one—medicine lodge or hermetic circle. Or dual natured watch-critters that look on the astral presence of an intruding mage as the magical equivalent of meals on wheels. Or how about bound spirits or elementals, or wards, or the biggie—patrolling mages or shamans. Getting the picture yet?

Okay, I'm throwing this open for discussion. If you have any experience with astral or magical security, and how to defeat it, log on and sound off.]<<<<<
—Trevor (10:55:29/11-1-53)

>>>>>[You hit the major points in your list, Trevor, but you forgot watchers. Watcher spirits are much easier to summon and bind than elementals or full-blown spirits, and they do a heck of a job as magical watchdogs. Gaeatronics uses a typical setup. The nuke plant's a big, sprawling place, and covering the whole thing with guardian spirits

would exhaust too many shamans. Instead, they simply summon and bind one or two *real tough* spirits, and set them to patrol a central area. Then they call up a drekload of low-voltage watchers. The watchers look out for intruding astral presences. As soon as they spot something, they *go fetch the spirits*. Once the cavalry comes over the hill, the watchers scoot off to notify the mundane security people to come and clean up the mess. Effective, and much more cost-effective than binding enough powerful spirits to patrol the whole facility.]<<<<<
—Lace (02:11:22/11-9-53)

>>>>>[In Tir Tairngire the big thing is dual watch-beasts, particularly charmers like sirens.]<<<<<
—Sal (11:20:45/11-12-53)

>>>>>[Tir Tairngire. *Gawd*, what a weird fragging place. They've got fragging *firedrakes* down there, man, firedrakes as fragging guard animals.]<<<<<
—Barnaby Rudge (19:11:24/11-13-53)

>>>>>[Lots of corp facilities in the outlying areas of the sprawl use hell hounds. I know for a fact that the MCT depot north of the plex where they mothballed those old t-birds uses them. And I hear Yamatetsu's Integrated System Products facility down in Fort Lewis has a couple patrolling the grounds at night. I've said it before and I'll say it again; trained hell hounds make the ideal guard animal. Being dual natured, they can hit the spell worms coming in astrally and still fry the samurai coming in over the fence.]<<<<<
—Mars (14:18:11/11-15-53)

>>>>>[Layered defense is a big thing for astral security as well as physical. Most corps start off with wards on the doors and windows to separate the pros from the wannabes. Then they add a couple of hell hounds or other dual watch-critters, followed by another couple of wards, then maybe some watchers. The watchers usually have instructions to call in other security forces, for example, an elemental or two accompanied by mundane sec-guards to take care of the intruding mage's samurai back-up. Or they might just try to scrag the intruders themselves. This is the varsity: big-time elemental or spirit action, plus the possibility of combat mages.

Sure, astral defense doesn't come cheap. But the megacorps consider it just another cost of doing business.]<<<<<
—Maurice (23:26:10/11-29-53)

>>>>>[I know they're necessary, but I *hate* bringing mages along on a run. They scare me.]<<<<<
—Black Flag (00:27:01/11-30-53)

>>>>>[Magophobic, Blacky?]<<<<<
—Igor (02:36:41/12-1-53)

>>>>>[No, you dolt. I almost got cooked when our mage detonated. Having a mage along is like packing sweating dynamite.]<<<<<
—Black Flag (23:28:11/12-9-53)

>>>>>[??? Tell us the story.]<<<<<
—Keefe (11:36:29/12-10-53)

>>>>>[We were in the tribal lands, you don't have to know where, making a run on a research facility. While the rest of us hunkered down outside the fence keeping a lookout, our mage went astral to scope out the place. He checked out of his body, and everything looked normal. Then, with no warning, the mage's body just seemed to explode. I saw fire everywhere, and the next thing I know I'm waking up in a hospital bed. The mage is dead, of course, and two of my buddies bought the farm too. Me, I'm medium rare, but still alive.

Afterward, I tried to reconstruct events and this is how I think it shook out. The astral mage, drifting through the facility, runs into something too tough for him. Maybe they duke it out a bit, maybe he catches it on the first exchange. Anyway, somebody or something slams a fireball or some other bad spell into our mage's astral body, and the spell "grounds" into the mage's *physical* body. While we squat around, waiting for him to come back and report, the guy's meat body suddenly becomes ground zero for a fireball. Next time I take a mage along, I'm going to lock him in a fragging blast-proof *box*.]<<<<<
—Black Flag (12:21:01/12-10-53)

>>>>>[Black Flag raises a valid point. Going into a situation astrally represents a certain risk to those guarding your body. An "astral sniper" can easily put a spell into your astral body and cook the rest of the team, as happened to Black Flag.

But for a mage, going in physically in an effort not to alert astral guardians also represents a risk. Most mages, whether hermetic or shamanic, carry fetishes or foci, which also have an astral presence. Theoretically, that same astral sniper could pump a fireball into the astral presence of a power focus, and that focus becomes the epicenter of the spell in the real world.

Disturbing? Yes. But nobody promised life would be easy.]<<<<<
—Trevor (15:12:51/12-20-53)
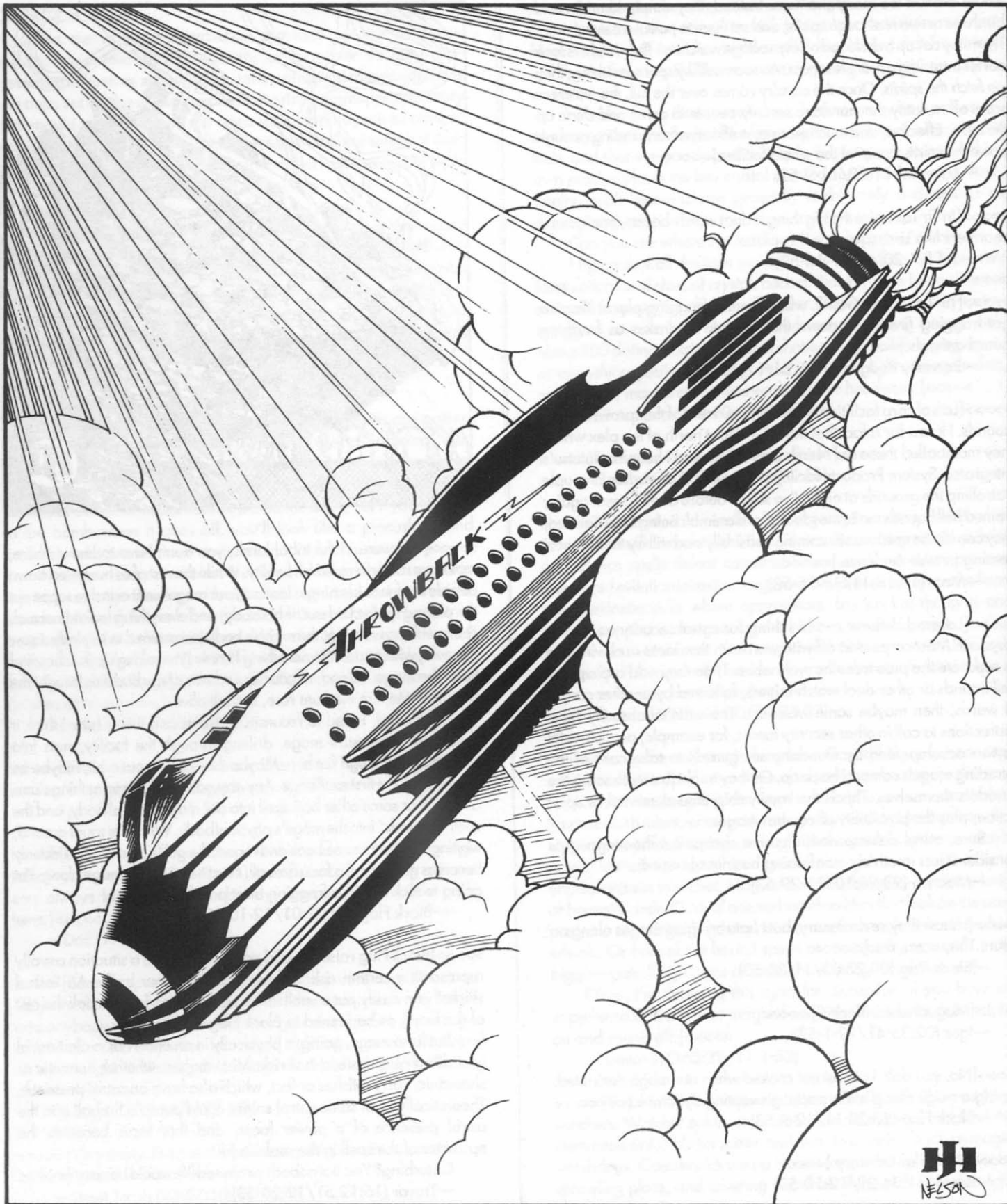
FRINGE OF SPACE

Reprinted from Discoveries, *a science publication for high school students, Spring 2052*

very one of us has seen the big planes flying overhead, been startled by the loud *crack* that sometimes echoes down from above the clouds, and heard the noisy *roar* as they land or take off at the airport. Some of us have even traveled by air to exciting places. Most people, however, only see them as big, white, dart-shaped objects, winging their way overhead.

>>>>>[Some people out there still seem totally mystified by any transportation technology more advanced than a power skateboard. This article on suborbitals and semiballistics should reach even them. Enjoy.]<<<<<
   —Captain Chaos (19:10:51/1-7-53)

THE PLANES

Three types of fast passenger planes fly in our skies today: semiballistics, suborbitals, and high speed civil transports (HSCTs).

SEMIBALLISTICS

Semiballistics take their name from the way they use rocket boost and the earth's atmosphere to fly. They travel the same path a stone would travel if thrown into the sky at the same speed and angle as the airliner. Semiballistics have wings, but use them to maneuver only during reentry and landing. At the midpoint of its flight, a semiballistic plane is too high up for the existing atmosphere to lift the wings.

A semiballistic plane takes off like a normal plane, but uses only some of its engines for liftoff. As soon as it clears the ground and moves a regulation distance from the city, it angles its nose until the plane is standing almost on its tail, then fires high-power engines to throw itself out almost to earth orbit. As it flies upward,

gravity pulls on it and slows it down. When the force of gravity drags it to a stop, the plane begins to fall back toward the Earth.

Naturally, the plane does not blast straight up. If it did, it would come down almost where it took off. It moves forward as well, tracing out a curve called a *parabola*. While the plane is in flight, the earth continues to turn beneath it, which makes planning and navigating a semiballistic flight very complicated.

>>>>>[Interestingly enough, semiballistics (SBs) use flight profiles similar to the old ICBMs the superpowers threatened each other with not so very long ago. I guess the SB developers benefited from all the research done on ballistic missiles, tracking, and so on.]<<<<<
—Cooper (13:28:27/2-11-53)

Once the semiballistic returns to the atmosphere, it uses its wings to slow down and enters the landing, or "terminal guidance phase," of its flight. Semiballistics land much faster than any other kind of plane in the history of flight. When a semiballistic plane comes in over the end of the runway, called the "threshold," it is traveling at about 300 kilometers per hour! A semiballistic uses up nearly all its fuel to boost itself above the atmosphere. When it lands, it has almost no fuel left.

>>>>>[This brings up a very interesting point: an SB gets one try at landing. It can't be stacked up in a holding pattern; it either lands or it crashes, and there's simply no other option. Think about that the next time you ride the old semiballistic "missile." If a private puddle-jumper is sitting on the runway the missile's scheduled to use, the two planes will merge.]<<<<<
—Flyboy (07:14:41/3-10-53)

>>>>>[I've heard that if hermetics or shamans leave the atmosphere they die or go mad. I'm a mage and I'm planning a trip to Tokyo. Should I ride the SB?]<<<<<
—WizKid (13:28:49/3-29-53)

>>>>>[I wouldn't recommend it, Wiz. The airlines just laugh off the concept of any risk, and I've never heard of any case where somebody suffered, but then again I've never known a mage to ride the missile. Maybe they're paranoid, or maybe they know something I don't. But I'd advise the suborbital.]<<<<<
—Flyboy (04:58:50/4-1-53)

>>>>>[A couple of mages *did* buy the farm aboard SB "missile" shots, but the airlines, predictably, buried the stories. However, many mages have ridden the missile safely. Make of that what you will.]<<<<<
—Russel (13:52:59/4-10-53)

>>>>>[How about checking with an expert, eh?—I'm glad you asked. Magicians, that's mages and shamans both, and I assume mystics of other disciplines, only face danger if they connect with astral space *in any manner* when beyond the Earth's atmosphere. I've gone up and come down a few times with no problems. Yes, some magicians have in fact died or gone mad on an SB trip, but to the best of my knowledge *all* attempted some kind of magic or astral perception/projection. They paid the price.

And by the way, don't carry any active magic items on an SB flight. You may find them drained of energy around the midpoint of the trip.]
—Sharpe (09:11:41/4-13-53)

TRANSCONTINENTAL PATHS

Suborbital

Semiballistic

Tokyo

= Gaiasphere

Seattle
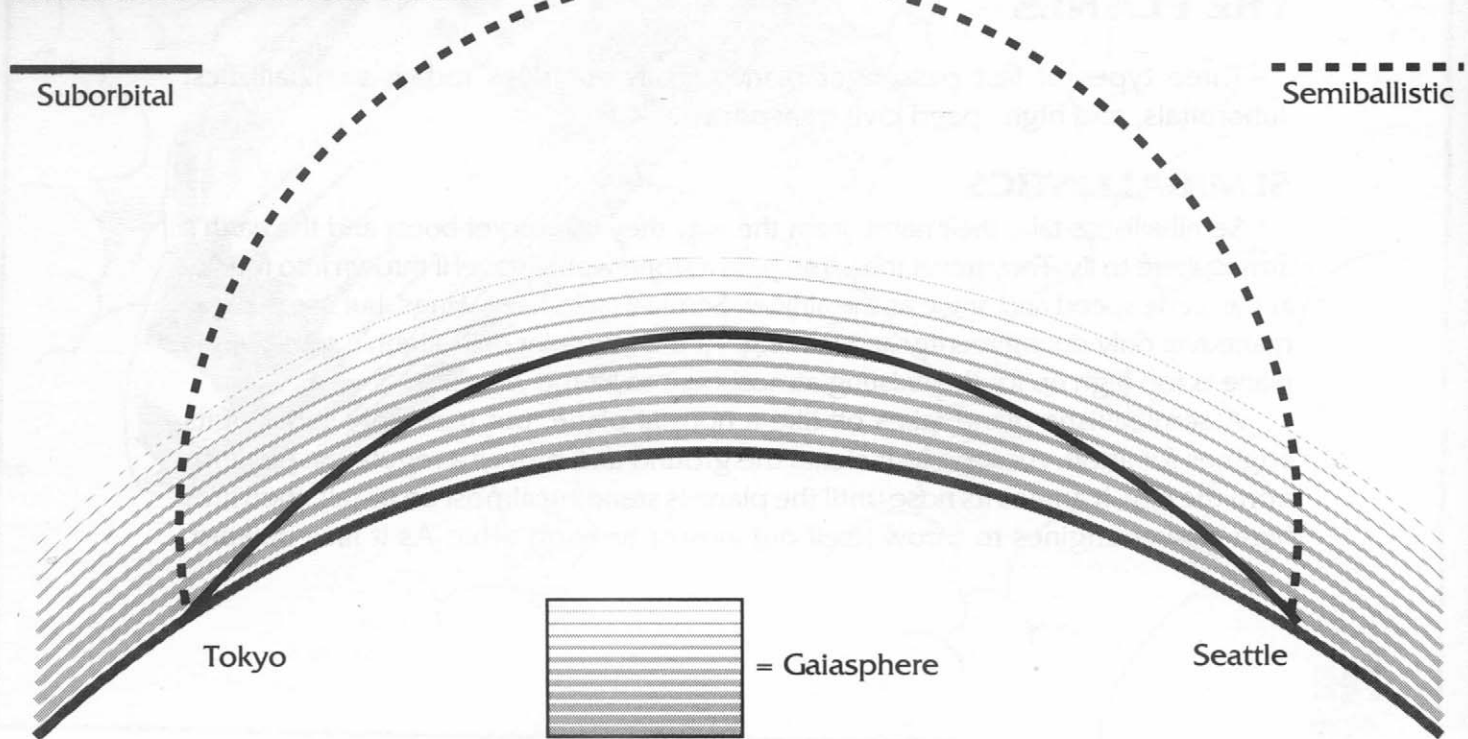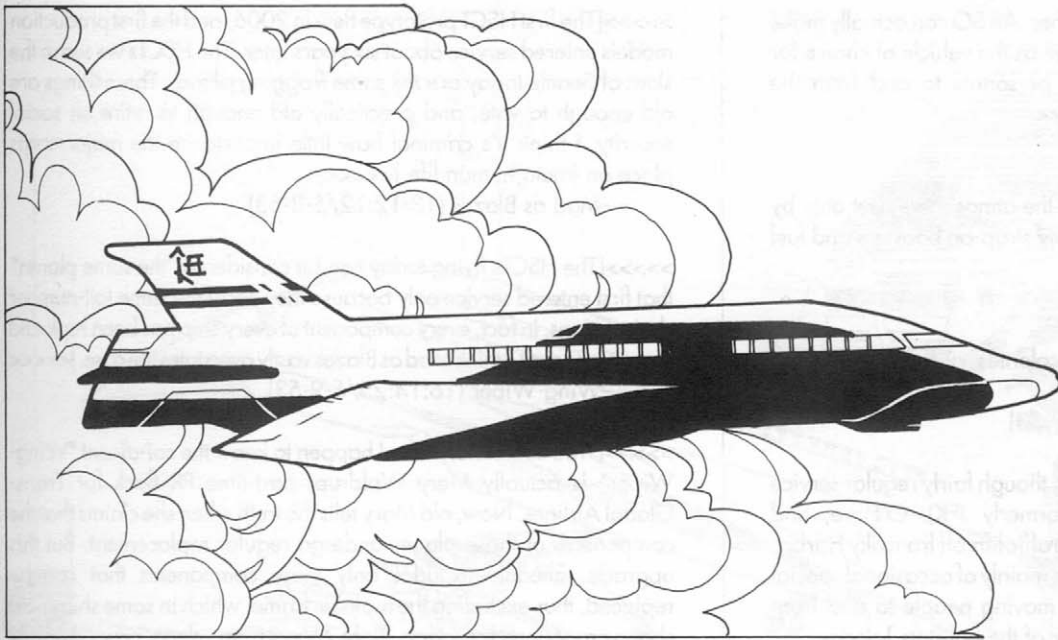
>>>>>[Say, that reminds me of a question I've been meaning to ask: what happens when an astrally projecting magician travels so high he or she starts to leave the atmosphere? I've heard the astral self can't leave the planet. What's the beat?]<<<<<
—New Snoop (21:12:31/4-23-53)

>>>>>[I know of no one who has successfully "left the planet" via astral space. I tried it once. As I rose above the living earth, I felt the astral plane grow decidedly colder, but I know astral space has no heat. What was it I felt, then? As I climbed higher, traveling at the speed of thought, my mind began to speak of terrible things. Above me I saw a great darkness, and all my fears combined descended upon me. I could not go on. As I allowed myself to fall, I looked upon the darkness, and in it I thought I saw movement…

But I can't be sure. I believe I may have gone temporarily insane—I don't know. I am not a scientist. But I will not repeat the experiment.]<<<<<
—Sharpe (08:31:47/4-24-53)

>>>>>[I hate to say it, but I think ol' Sharpe ain't what he used to be. I've gone high too, chummers, and there's *nothing* up there, and I mean that literally. Nothing at all beyond Earth's biosphere. Zip. Nada. Squat. Nothing. Void.

As for the magicians who go nuts in outer space: here's what I think happens. Imagine holding a balloon full of air (the magician) in a vacuum (where astral space would be, beyond the earth, except *nothing* is there). Now, prick a small hole in the balloon to simulate the magician connecting to astral space to cast magic, or whatever. What happens? All the air in the balloon (the energy in the magician) rushes out into the vacuum. Oops.

It's that simple, chummers. Nothin' else.]<<<<<
—Evaine (17:56:29/4-25-53)

SUBORBITALS

Suborbital planes fly much like normal planes or HSCTs. They take off like standard planes, and like semiballistics, fly relatively low and slow until they have cleared the city. Then they fire powerful engines called SCRAMjets to accelerate and climb. While semiballistics travel so high that they are effectively in space, suborbitals fly at altitudes of about 75,000 feet, or 23 kilometers. The air at this altitude is too thin to breathe unaided, but the air remaining in the atmosphere creates enough friction to raise the temperature of the plane's "skin" to almost 400 degrees Celsius!

Unlike semiballistics, the suborbital pilots have complete aerodynamic control of the plane throughout the flight. The pilot can change the destination of a suborbital in mid-flight, or even turn around and head back (if the plane carries enough fuel). A semiballistic's course, by contrast, is calculated before takeoff and cannot be changed en route.

>>>>>[So SOs *can* stack up in holding patterns, and *can* make a second try if they have to wave off an approach. In fact, SO pilots practice touch-and-go landings out in the Yakima tribal lands: they come in on final approach and touch the wheels down, then pour on the power, pull back on the stick, and climb out to try it all over again.]<<<<<
—Flyboy (07:19:15/3-10-53)

>>>>>[Today's suborbitals originated in research done by the U.S.A. (when that still meant something) and Germany (ditto). The Americans called their project the Orient Express, and the Germans named theirs the Saenger.]<<<<<
—Clifton (05:02:53/3-14-53)

>>>>>[Just for the record, magicians face no danger at all from suborbital flights; the aircraft don't climb high enough to reach a danger zone. The airline, though, might still take exception to any magical activity....]<<<<<
—Sharpe (08:47:31/4-24-53)

>>>>>["Suborbital" is kind of a misnomer. An SO can actually make the lift to low-earth orbit, and they serve as the vehicle of choice for corporations transferring goods and personnel to and from the habitats and colonies "up there."]<<<<<
—Zingbat (15:28:09/4-25-53)

>>>>>[An SO *can* make the lift out of the atmosphere, but only by adding some pretty-fragging-heavy-duty strap-on boosters and fuel tanks.]<<<<<
—Flyboy (10:28:10/4-26-53)

>>>>>[Is there much traffic to the colonies and habitats from SeaTac?]<<<<<
—Out-of-Towner (05:30:11/4-29-53)

>>>>>[No regular service from SeaTac, though fairly regular service runs out of Kennedy International (formerly JFK), O'Hare, and Dallas/Fort Worth. Somewhat regular traffic lifts off from Sky Harbor in Phoenix. Rare lifts from SeaTac consist mainly of occasional special flights on corp-owned SOs, aimed at moving people to and from Zurich-Orbital, or occasionally another of the habitats.]<<<<<
—Blaine (15:33:47/5-1-53)

>>>>>[Couple years back, one of Aztechnology's experimental habitats—the one they call "the Spindle"—had major problems, and the big A needed to relocate their people groundside in a big fragging hurry. SeaTac handled three lifts in twelve hours, more than they usually handle in a month.]<<<<<
—Waverly (19:44:57/5-2-53)

>>>>>[I need to make a lift to Zurich-Orbital for a run. How can I do it?]<<<<<
—Sly (03:36:41/6-28-53)

>>>>>[Quick answer: you can't. No passenger service exists, so you can't just buy a ticket. Best bet, get a corp to certify you as an authorized passenger. But make sure the authorization's absolutely datatight—no simple faked pass will get you past SO security. And don't even think about stowing away; weight for a lift is accounted for down to the gram. You could try bribing an officer, but there's no guarantee he'd *stay* bribed, and you might end up breathing vacuum outside an airlock. It's a tough gig, Sly. If you make it, let me know how you did it. It'll make a heckuva good story.]<<<<<
—Sten (11:25:57/6-28-53)

HSCTs

The high speed civil transport developed as a result of research carried out by the United States of America at the end of the last century. A long, slender, and beautiful design based on the first supersonic passenger plane, the Concorde, the HSCT is often called "the son of Concorde." The HSCT flies like a standard plane, rarely climbing above 60,000 feet, or 18 kilometers. Powered by eight multi-phase, multi-mode engines that operate as turbofans on takeoff and landing, the engines switch to turbojet operation for high cruising speed.

>>>>>[The first HSCT prototype flew in 2006, and the first production models entered service about six years later. The HSCTs we see in the skies of Seattle today are *the same fragging planes*. These things are old enough to vote, and practically old enough to retire on social security. I think it's criminal how little importance the major corps place on (meta)human life.]<<<<<
—Mad as Blazes (13:12:12/5-8-53)

>>>>>[The HSCTs flying today can be considered "the same planes" that first entered service only because they carry the same tail-number designations. In fact, every component of every ship has been replaced many times over. I think Mad as Blazes vastly overstates the case.]<<<<<
—Wing-Wiper (16:14:25/5-9-53)

>>>>>[True confession time. I happen to know the *soi-disant* "Wing-Wiper" is actually Mary Waldrup, part-time PR flack for Trans-Global Airlines. Now, old Mary tells the truth when she claims that the components of those planes undergo regular replacement. But this upgrade schedule includes only those components that *can* be replaced, thus excluding the main airframe, which in some ships now shows pronounced cracking. Right, Mary? Come clean, now...]<<<<<
—Skeleton Hunter (23:52:18/5-25-53)

THE SERVICE

Though each type of plane offers a different kind of flight, most airlines provide the same or similar services. The differences lie in the speed of the trip, the ticket price, seat class, and other features.

HOW FAST IS FAST?

Modern planes fly far faster than older forms of air travel. The fastest of the semiballistics travel at Mach 30, which means 30 times the speed of sound, or almost *35,000 kmh* (almost 22,000 mph)! Suborbitals move slightly slower, traveling at 25 times the speed of sound, or 29,000 kmh. The slowest modern passenger plane, the HSCT, travels at only three times the speed of sound, or about 3,500 kmh. Even this "slow" plane flies a lot faster than any plane from the last century.

As an example of just how fast planes travel in this modern age, an HSCT traverses the distance from Seattle to Tokyo in little more than four hours. A semiballistic or suborbital flight between those two cities takes less than an hour. That's fast!

PRICE OF A TICKET

Air travel traditionally costs more than any other form of transport. However, even though today we travel much faster than our parents did, we pay only slightly more than our *grandparents* did. For example, it costs approximately 2,000¥ to fly from Seattle to Tokyo on an HSCT, and about 2,500¥ for a semiballistic or suborbital flight.

>>>>>[Which means that the HSCT carriers operate at a loss. According to some figures I dug up, the operating cost for an HSCT is about .1¥ per passenger kilometer. An HSCT carries 300 passengers. On a two-thirds-full flight, that's 200 passengers, each paying

2,000¥, for a total of 400,000¥. We'll say the Seattle-Tokyo trip is 14,000 klicks for a nice round number, or 4.2 million passenger kilometers. At .1¥ per passenger klick, it costs 420,000¥ to make the hop, but they're bringing in only 400,000¥.]<<<<<
—Lavin (11:57:39/4-12-53)

>>>>>[Yeah, well, they more than make it back on the SO and SB flights, let me tell you. A suborbital costs about .5¥ per passenger kilometer, and a semiballistic costs even less. At a ticket price of 2,500¥ for Seattle to Tokyo, the carriers just *rake*.]<<<<<
—The Keynesian Kid (00:11:59/2-28-53)

YOUR PILOT AND CREW

Even today, most people still consider an airline pilot's job fun and glamorous. That may have been true in the past, when pilots actually controlled the plane and the fate of the passengers. Today's pilots wear vehicle control rigs, no longer flying the planes using physical controls but "jacking in" to the planes' computerized systems. Most suborbitals, semiballistics, and HSCTs carry a pilot and copilot, only one of whom is jacked in at any time. If necessary, the plane's computerized autopilot can also take complete control of the plane and bring it in for a safe landing.

Flight attendants care for the passengers' personal needs, serve refreshments, and ensure that everyone aboard the plane observes safety precautions during the flight.

>>>>>[Don't discount the stewards and stewardesses just because they wear lame outfits and spend most of their time serving lousy champagne in first class. When commercial air travel began more than a century back, the crew included "flight attendants" whose only job was safety: they made sure people buckled up, and got them off safely if the plane went down.

Predictably, knowing why the cool-eyed attendants were *really* there kinda scared the pee out of the passengers. The airline owners responded by changing stewards to stewardesses, dressing them up in skimpy outfits, and generally using them as glorified cocktail waitresses. Of course, these transformed flight attendants were just as well-trained as their predecessors, but people could view them differently.

Recently, this transformation took place again, this time swinging in the opposite direction. Modern flight attendants are still responsible for passenger safety, and today that means more than making sure passengers fasten their seatbelts. Flight attendants must excel at various forms of lethal and non-lethal combat, armed and unarmed. Because bullets may punch holes in the fuselage and depressurize the plane, flight attendants don't carry firearms. But depending on the policies of the airline, most wear or carry shock gloves, stun batons, and/or tasers.

Sure makes you see the little fellow serving you your midflight martini in a different light, doesn't it?]<<<<<
—Jason (15:04:50/10-15-53)

KILLER ACCESSORIES

Reprinted from Ascending: The DataMag for the Upwardly Mobile, *Spring 2050*

I n today's world of high tech and higher expectations, even top executives will not win the Big Prize just by getting the job done. The job must be done *in style*. This axiom holds as true for negotiating a social merger over a pint of pure-brewed ale at Noggins Brew Pub as it does for facing down a hostile board of directors. *Everything* about today's up-and-comers has to convey their personal style—the *right* style.

Everything, including your personal defense options. One day out of a thousand you will need them to protect yourself; the other nine hundred and ninety-nine, they serve as accessories the same as your AST pocket comp or Haliburton briefcase.

To help you match your personal defense to the rest of your personal style, we present ten options our evaluators judged as the best blend of flash and function.

>>>>>[My oh my, "personal defense options." I guess good, old-fashioned, to-the-point words like "weapons" are out of fashion this season...

If anyone out there has had experience with any of these things (from either side of the grip), please jump in and enlighten the rest of us. I realize it's unlikely that anyone reading this BBS has actually laid out the nuyen to *buy* any of these gadgets...so if you happen to own one, *don't* tell me how you acquired it. Thank you.]<<<<<
—Captain Chaos (17:01:06/1-11-52)

FICHETTI TIFFANI NEEDLER

Fichetti Firearms does it again. Fichetti produced last season's ultra-fashionable yet effective Self-Defender personal pistol. This year's model, the Tiffani Needler, updates the styling and color selection and upgrades the technology. Fichetti decreased the round caliber to 1.5mm, but made the needle rounds* explosive to increase stopping power.

	Type/Conceal	Ammo	Mode	Damage	Weight	Avail	Cost	Street Index
Tiffani Needler	Hold-out/8	4 (c)	SA	4L1 (5L)	.5	7/48 hrs	650¥	2

*Though similar to flechette rounds, needle rounds do not use flechette ammo rules. Designed to penetrate, rather than shred and tear like flechette rounds, characters use Impact Armor to defend against needle rounds rather than Ballistic Armor as for standard rounds. Needle rounds *will not* penetrate Impact Armor with a Rating of 3 or greater as the rigid plating in these types of armors stops needle rounds. Needle rounds are useless against vehicles in all situations.

Needle ammo can be purchased for all classes of firearms at double the cost of regular rounds. Needle ammo uses the same Damage Code as the weapon's standard ammo, but may not be combined with other types of ammo.

>>>>>[Notice how they discuss new styling and colors before mentioning a significant change—in fact, an improvement—in technology? Shows you where this rag's focus lies. Guns in this year's power colors, gawd...]<<<<<
—Frankie (17:25:03/1-28-53)

BARTON ARMS GUN CANE

A perfectly-balanced walking stick...but with a lethal difference. The Barton gun cane has an artificial ivory handle in the familiar "pistol grip" style used for walking sticks since time immemorial. With the Barton, however, style meets function. A quick press of the thumb on a recessed stud primes the weapon; an easy squeeze with the index finger fires a single 8mm hollow-point round from the tip of the cane. Perfect for that once-in-a-lifetime surprise!

	Type/Conceal	Ammo	Mode	Damage	Weight	Avail	Cost	Street Index
Gun Cane	*/2/9**	1	SS	3M2 (6L)	1	10/7 days	500¥	2

*Use Hold-Out Pistol ranges for this weapon.

**Use the first number if attempting to conceal the entire cane (e.g., under a duster); use the second number to determine how easy it is for someone to notice the weapon mechanism within the cane.

>>>>>[Ya know, I kind of like this idea, flaky though it sounds. Range and accuracy are predictably poor, but it's not for sniping anyway. More likely you'll be cramming it into the belly of a would-be mugger...or a security guard, for that matter. Reload the gun by unscrewing the lower 15 centimeters of the cane and mounting another round in the chamber.]<<<<<
—Kingfisher (04:15:45/2-20-53)

BARTON ARMS BRACER

Another fashion hit from world-renowned Barton Arms! The ultimate hold-out weapon, the Bracer looks like a beautiful piece of jewelry, a massive bracelet of titanium polished to bring out its natural blue color and crystalline structure. Built into the Bracer next to the latch, which lies against the underside of the wrist, is a single-shot mechanism designed to fire a single hollow-point round. The wearer arms the weapon by sliding part of the design on the latch, and fires it by bending the hand back to free the muzzle. The bracelet is an original design by Bartellucci.

	Type/Conceal	Ammo	Mode	Damage	Weight	Avail	Cost	Street Index
Bracer	Hold-Out*/7**	1	SS	3M2 (6L)	.3	12/7 days	1,300¥	3

*Increase all base target numbers by 1.
**Refers to the concealability of the weapon mechanism.

>>>>>[Same firing mechanism as the gun cane, above. This weapon provides *no* barrel whatsoever, so accuracy is pretty damn lousy. I saw a corp-scag fire one of these at what she thought was a go-ganger, miss by a mile, then yell bloody blue murder because the muzzle flash burned her wrist.]<<<<<
—Kingfisher (04:20:29/2-20-53)

MORRISSEY ÉLAN

The smallest of Atlanta-based Morrissey Manufacturing's new line of personal defense options, the Élan displays a refreshing style all its own. Like many modern weapons, the Élan is constructed mostly of polyresin. While other polyresin pistols retain the blocky "automatic pistol" shape that initially stemmed from the machining processes required to produce metal parts, the Élan uses polyresin's true potential to produce a hold-out both stunning in appearance and effective.

	Type/Conceal	Ammo	Mode	Damage	Weight	Avail	Cost	Street Index
Élan	Hold-Out/8	5 (c)*	SA	4L1 (5L)	.5	8/7 days	500¥	2

*The Morrissey Élan pistol cannot fire flechette or needle ammo.

>>>>>[The first time I had one of these pointed at me it took me a second or two to even recognize it as a gun. It looks like a plastic toy pistol left in the sun too long or stuffed in a microwave and half-melted.

Anyway, I lifted it from the suit impolite enough to stick it in my face and put it through its paces myself. It's actually a nice piece of ordnance. It packs a little more punch than your standard hold-out, and produces negligible recoil. It can't fire flechette rounds, though, a serious disadvantage.]<<<<<
—Bullyboy Grim (09:53:49/1-31-53)

DANA KNUTSON 92

MORRISSEY ELITE

The second entry in the Morrissey line, the Elite brings to light pistols the same sense of style that the Élan gives hold-out pistols. The Elite ups the ante on other lights by incorporating an under-barrel integral laser sight and increasing the size of the round. The Morrissey Elite lets you take 'em down in style!

	Type/Conceal	Ammo	Mode	Damage	Weight	Avail	Cost	Street Index
Elite	Heavy*/6	5 (c)	SA	4M2 (9M)	1	6/48 hrs	950¥	2

*Though the weapon fires heavy-pistol ammunition, it uses light-pistol ranges.

>>>>>[Same melted-plastic look as the Élan.]<<<<<
  —Bullyboy Grim (09:59:08/1-31-53)

>>>>>[The tech's better, though. The laser is reliable, and difficult to knock out of alignment. Because the Elite chambers heavy-pistol ammo, you can use the wizzer special-purpose rounds like APDS. If you're into blowing *big* holes in things (and who isn't?), consider APDS/explosive, and so on...]<<<<<
  —Winger (13:09:07/2-19-53)

MORRISSEY ALTA

The top of Morrissey's new line, the Alta heavy pistol has no peer. The Alta provides the same dependable laser sight as the Elite, and includes Morrissey's proprietary chamber mechanism for outstanding mechanical reliability. Serious stopping power with serious style: the Morrissey Alta!

	Type/Conceal	Ammo	Mode	Damage	Weight	Avail	Cost	Street Index
Alta	Heavy/6	12 (c)	SA	4M2 (9M)	1	8/48 hrs	1,200¥	2

>>>>>[A *big* chunk of melted plastic.]<<<<<
  —Bullyboy Grim (10:03:52/1-31-53)

>>>>>[Morrissey's style-over-substance attitude prevented them from adding any kind of recoil compensation to this puppy. Too bad: it doesn't mass much for a heavy pistol, so most of the recoil transfers right into all those tiny bones in your wrist. Suppose Morrissey also sells designer braces for sprained wrists?]<<<<<
  —Yobo (16:40:14/2-18-53)

RAECOR STING

An innovative hold-out, the Sting is Raecor's own "lemon-squeezer" model, designed to be held in the fist with the short barrel extending out between the index and second fingers. To fire the Sting, squeeze the fist, and the unique circular magazine rotates to bring the next mini-flechette round into place. Constructed exclusively from high-temperature polyresins, the Sting cannot be detected by standard metal scanners.

	Type/Conceal	Ammo	Mode	Damage	Weight	Avail	Cost	Street Index
Sting	Hold-Out/9	5 (c)	SS	2L1 (4M(f))	.25	10/7 days	375¥	2

>>>>>[Couple of points. First, Raecor didn't invent the lemon-squeezer design. An assassin used a similar weapon to geek some American president, I can never remember which one, back a couple hundred years. Second, modern weapon detectors don't just detect metal; a chem-sniffer will probably pick up the propellant in the rounds.]<<<<<
        —Diz (10:42:55/2-26-53)

>>>>>[Effective little beast, but be forewarned. The Sting accepts only its own specialized ammo, which isn't always easy to track down.]<<<<<
        —Marlin (06:04:06/8-7-53)

EICHIRO HATAMOTO II

The Hatamoto from Eichiro Corporation of Kyoto has topped the list among Japanese corporators for almost a year. Now the Hatamoto II—fully redesigned for 2053—has arrived in Seattle!

The Hatamoto is a single-shot, large-bore, personal defense option designed for high-threat situations where subtlety no longer matters. The polyresin body, available in a dozen designer colors, features a wraparound grip with a wrist brace to minimize recoil effects.

When the talking's done, trust the Hatamoto II to give you the last word.

	Type/Conceal	Ammo	Mode	Damage	Weight	Avail	Cost	Street Index
Hatamoto II	Shotgun/6	1	SS	3M3 (8S)	2.5	12/7 days	1,200¥	2

>>>>>[Think of it, boys and girls. Corp suits roaming the streets of our fine city packing single-shot handguns chambered for *shotgun* rounds! Kinda makes you want to walk a little softer, don't it?]<<<<<
        —Chuckie (10:53:08/3-14-53)

>>>>>[Keep in mind that this thing *looks* like a pistol. (A pistol with a weird grip, granted, but a pistol nonetheless.) So you might be tempted to trust your armor to stop a slug or two when you make your move. Maybe your armor *will* stop a heavy pistol round, but will it cope with this joker at pointblank range? I strongly advise you to learn to recognize the grip-and-wrist-brace arrangement of this toy on sight and give it the respect it deserves.]<<<<<
        —Lucky Luke (03:25:56/3-25-53)

>>>>>[The wraparound grip and wrist brace are absolutely necessary. This thing uses the same ammo as a Defiance T-250, but masses like a heavy pistol. Without the weapon mass to absorb it, the recoil goes right where you'd guess.]<<<<<
        —Denny (13:11:41/4-27-53)

SHARPEN YOUR IMAGE

REAL LIFE

ILLUSTRATED BY JOEL BISKE & JIM NELSON • COMPUTER DIAGRAMS AND ILLUSTRATIONS BY MIKE NIELSEN

ARMANTÉ

FIRING STUD

BARTON
ARMS
GUN
CANE

SCREW - OFF TIP ALLOWS
EASY LOADING AND CLEANING

TRIGGER FIRING FIRING   BARREL
FUSES   BOX   PIN   PG. 30
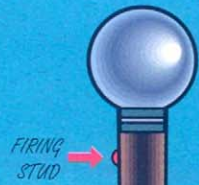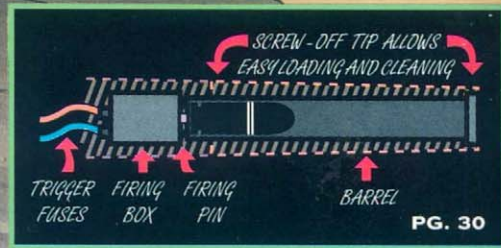
EICHIRO HATAMOTO II   PG. 32

ARMANTÉ
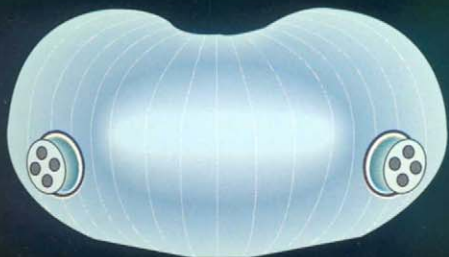
FELLINI-MED
BREATHER PG. 74
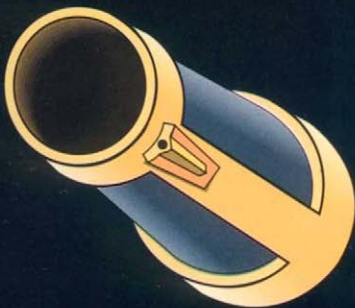
BARTON ARMS
BRACER PG. 30

STANLEY
'SCREAMER' PG. 74
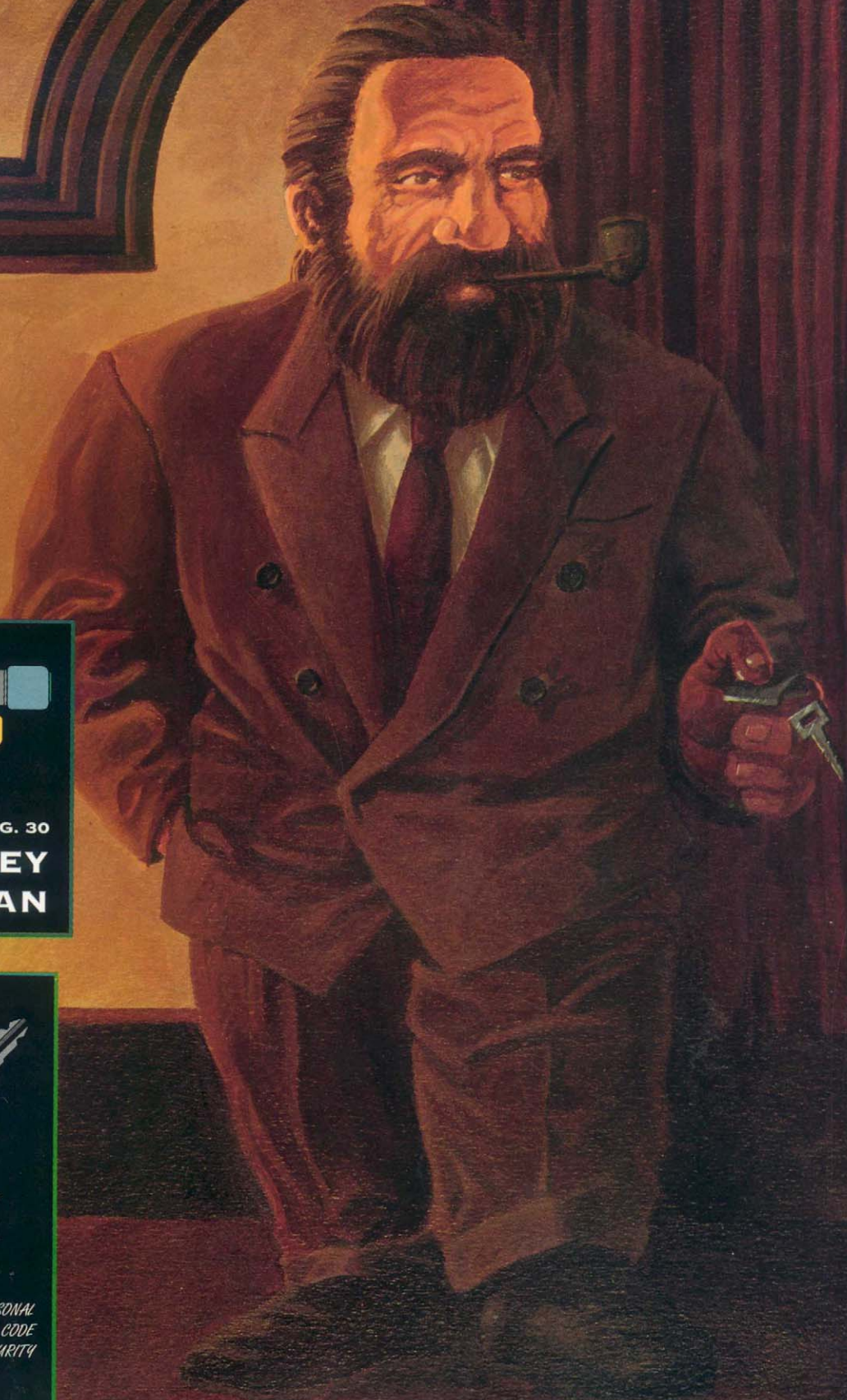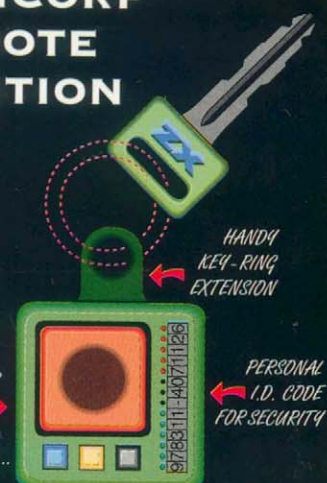
AUDIO SCAN IN PROGRESS...

VASHON ISLAND
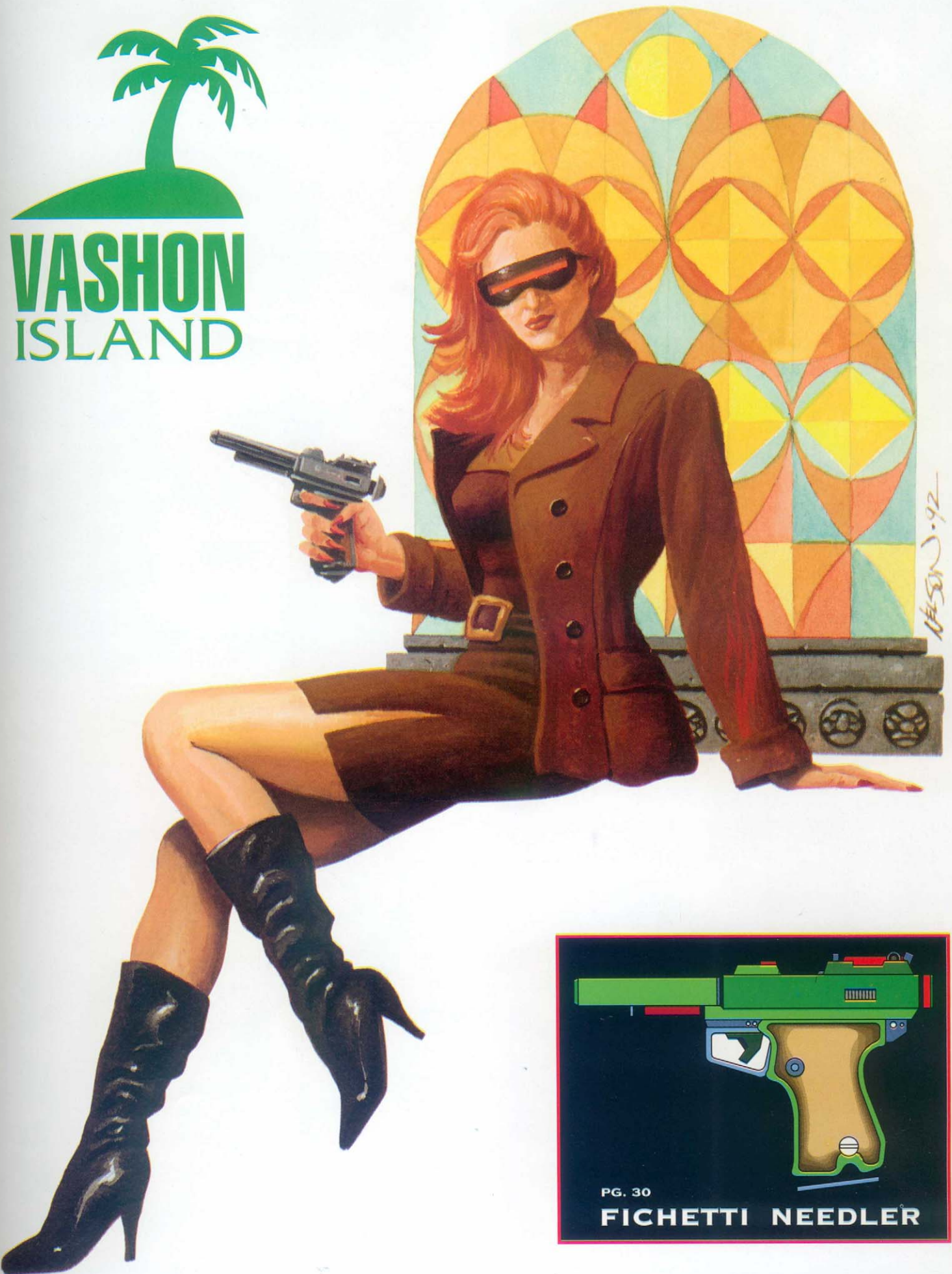
PG. 30
FICHETTI NEEDLER

MORTIMER OF LONDON

YAMAHA PULSAR PG. 33

MORRISEY ALTA PG. 31

ZOÉ

PG. 32
RAECOR STING

DATA DISPLAY

SENSORY ADJUSTMENT CONTROLS

TARGET: 43 METERS
SPEED: 43 KPH
SPECIES: TROLL

SOFT-TOUCH ADHESIVE BAND

SLEEK (NON-ALLERGITIC) STEEL-ALLOY FRAME

WHITELAW ELECTRIC SUNGLASSES PG. 73

WHITE NOISE MICROPROCESSOR

STANDARD EARRING

TOSHIBA WHITE NOISE GENERATOR PG. 75
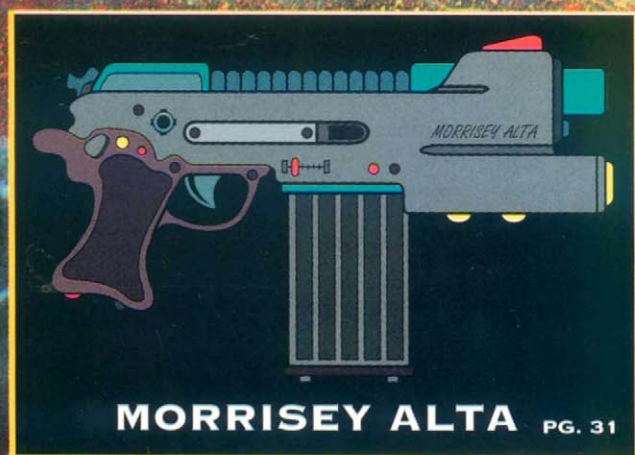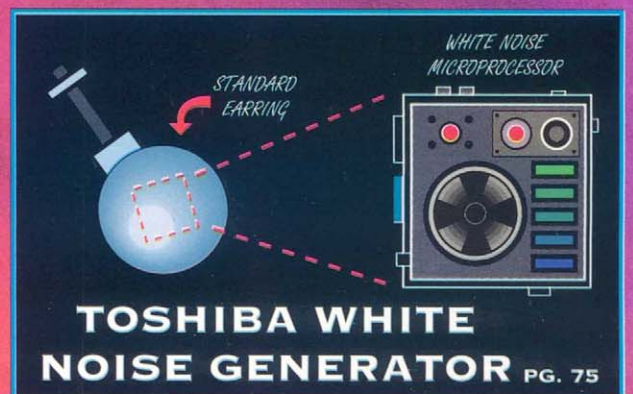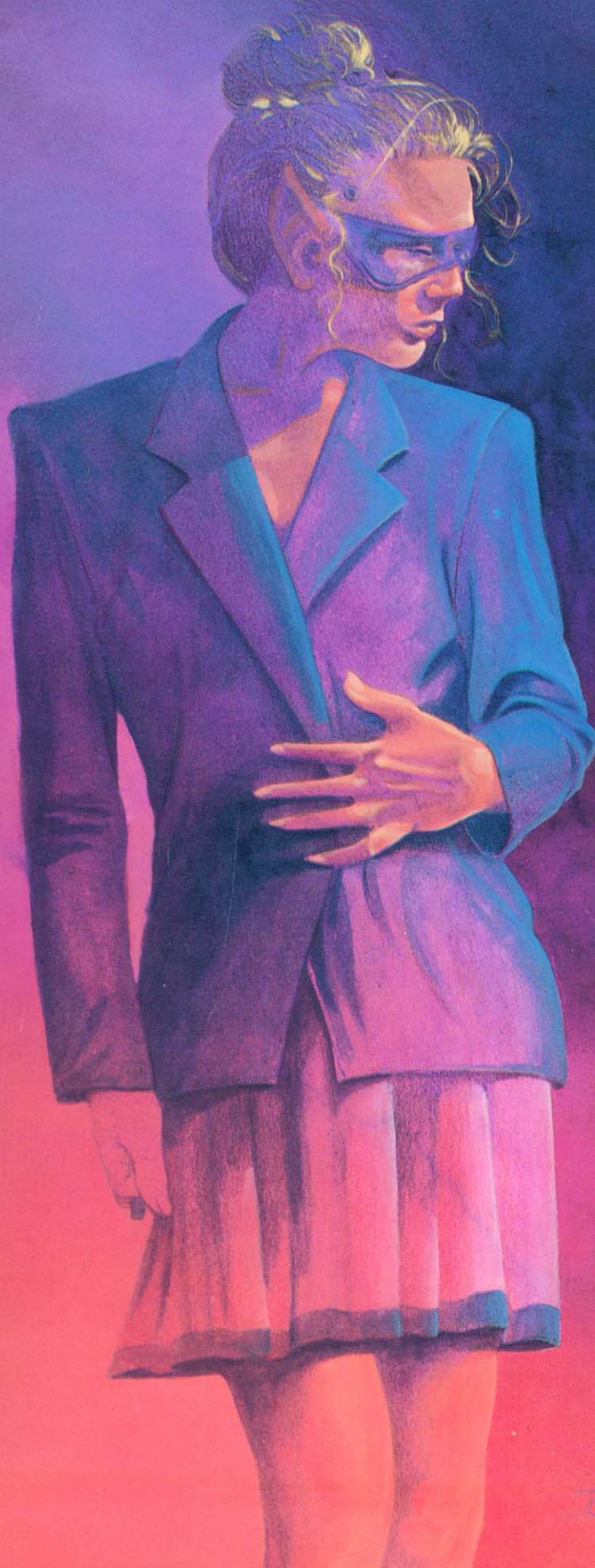
ZOÉ

FICHETTI
'EXECUTIVE
ACTION' PG. 33

FICHETTI EXECUTIVE ACTION

While others debate, executives take action! With that winning mentality in mind, Fichetti created the Executive Action light pistol.

Extensive research proves that the first three rounds of a multi-round burst are the most accurate; then recoil throws the weapon off true. Fichetti designed the Executive Action to solve this problem; it limits autofire to three rounds and triggers these rounds so quickly that the muzzle doesn't have time to rise. A single stroke of the trigger fires three rounds at an astounding cyclical rate of *50 rounds per second*. Three rounds exit the barrel in less than .1 seconds, guaranteeing the tightest shot grouping of any autofire pistol on the market.

	Type/Conceal	Ammo	Mode	Damage	Weight	Avail	Cost	Street Index
Exec. Action	Light/6	24 (c)	(SA/BF)	4M2 (6L)	1.5	14/7 days	1,150¥	3

>>>>>[Hey, this is a good idea! How did something that's actually useful on the street get into this fashion parade?]<<<<<
   —Dinger (19:11:40/2-25-53)

>>>>>[Check out the price, Dinger. Sure it's a good idea, but not at 1,150¥. I guess the people who read *Ascending* like to pay a premium for everything.]<<<<<
   —Prole (23:59:00/5-27-53)

>>>>>[Geeeeeeeeez, chummers, get with it: Beretta's had this deal on the market for three years now. Guess it took Fichetti this long to pirate the specs...]<<<<<
   —Finger (12:51:14/5-29-53)

YAMAHA PULSAR

Renowned innovator Yamaha brings striking new lines and (literally) stunning new technology to the taser. The Pulsar uses the capacitor-dart technology developed by Defiance, eliminating the trailing wires connecting the dart to the weapon and adding a twist. Instead of delivering a simple "flat" discharge, Pulsar darts modulate the discharge voltage in a sine-wave pattern, maximizing its disruptive effect on neural signals. A single Pulsar dart provides a clean, stylish way of preventing a confrontation from turning nasty.

	Type/Conceal	Ammo	Mode	Damage	Weight	Avail	Cost	Street Index
Pulsar	Taser/5	4 (m)	SA	8S2 (10S) Stun*	2	12/7 days	1,350¥	2

*If struck by a dart, the victim makes a Body Resistance Test using a Target Number of 10 to resist the effects. Unless the victim successfully resists the damage, he is incapacitated by muscle convulsions for 3D6 turns. The victim may reduce the number of turns of incapacitation by making a Body Resistance Test against Target Number 8. Each success reduces the number of turns of incapacitation by one.

>>>>>["Stunning new technology"—it's a taser. I get it. Ga-harf ga-harf...]<<<<<
   —Olympia (14:11:40/2-25-53)

>>>>>[At 1,350¥, this thing's vastly overpriced. But the sine-wave discharge *does* seem to work remarkably well.]<<<<<
   —Block Mother (14:29:25/3-4-53)

CLOSE OUT
CLEARANCE SA

DRESSED TO KILL

Reprinted from Century XXI: The Magazine of Style, *January 2053*

Century XXI readers keep their finger on the pulse of the fashion world. They know the up-and-coming trends and make them *theirs*, making their statement before everyone else jumps on the bandwagon. More importantly, they know what trends are out. Surprisingly, the latter knowledge seems lacking in many of the would-be stylish who, to be brutally honest, should simply know better.

The "street mercenary" look—obvious armor, *harshly* exaggerated silhouette, and utilitarian color scheme—provides a good example. The style first appeared in 2049 among the fashion leaders, then caught the popular imagination and quickly spread into the mainstream. By the middle of 2050, armored clothing—specifi-cally, armored clothing that *looked* like armored clothing—was *haute couture*.

Through the end of 2050 and into 2051, the style became progressively more exaggerated. Armored clothing began to copy the lines and textures of heavier armor. Shoulder pads hardened and extended, resembling the epaulets of a semi-rigid SWAT vest designed to protect the wearer's collarbones. Jacket and sweater fronts gained ridges reminiscent of rigid plating, and collars stretched upward to mimic the mounting ring for armored helmets.

>>>>>[High fashion has *never* made any sense to me. All these changes made clothes look more like serious armor, but did the actual armor protection of that clothing increase? *Nooo* sir, that wouldn't be fashionable. *Fake* armor is okay, *real* armor is gauche.]<<<<<
—Deirdre (16:31:18/5-15-53)

>>>>>[Not to mention illegal, in many sectors.]<<<<<
—Gene (11:37:23/6-7-53)

But this is 2052, people. The street merc look is *out*. In the vogue circles, street merc wear is *so* déclassé that as far as they're concerned it never happened.

Of course, just as trends move down the socioeconomic and status ladder, so does the realization that a trend has ended. So, even though *Century XXI* readers know that high fashion has turned to lighter, almost diaphanous, fabrics, softer silhouettes, and loose, flowing cuts, many of the would-be fashionable still dress as though looking for a friendly Saturday-night firefight.

>>>>>[Those of us who *are* looking for a friendly Saturday-night firefight take exception to the derogatory tone of that last statement.]<<<<<
—Blaze (05:44:45/5-24-53)

>>>>>[Sorry chummer, but if you really do spend your time looking for a fight you deserve all the derogatory comments you get.]<<<<<
—Vision Childe (12:51:43/5-27-53)

STYLE WITH SECURITY, SECURITY WITH STYLE

On the mean streets of the sprawl, "to die for" fashions frequently become just that. "Smartly dressed" today means clothes combining style and security.

Designers ranging from Armanté to Zoé accepted this fact of life, took the challenge, and, *Century XXI* is glad to announce, rose magnificently to the occasion. The well-dressed man or woman may choose from various styles of highly fashionable garb that smoothly combines protection, comfort, and practicality. The finest examples of this clothing style conceal their protective function almost perfectly. And for those occasions when wearing *any* armor simply *isn't done*, all armor sections detach easily and fold flat for storage. Here's a sneak preview of what the top designers have to offer this year.

ARMANTÉ

Armanté of Dallas currently offers the widest range of "secure" evening wear for men and women.

The designer's "Venetian" line of evening gowns and cocktail dresses brings back the "cloth-of-gold" look popular in the Renaissance era, when delicate threads of lustrous gold were woven into fabric. The shimmering effect created by the movement of the light cloth is difficult to describe but impossible to forget. The modern version of the "gold" thread, polymerized Crystle™ from DuPont, turns the fabric into a surprisingly effective ballistic cloth.

The "Starlight" line of evening gowns enhances the striking cloth-of-gold effect by sprinkling brilliant *faux* diamonds over the entire dress. In candlelight, the gown seems to glow. The *faux* diamonds consist of chemically modified cubic zirconium, scattered across the fabric in a way that provides considerable impact protection.

Of course, no evening ensemble is complete without a shawl. The Armanté design looks like raw silk, but the "*Ancien*" shawl incorporates the same Crystle™ threads as the dresses, providing additional ballistic protection for the wearer's back and shoulders.

Needless to say, Armanté doesn't neglect the gentleman. The "Executive Suite" suit brings the revered tuxedo style into the second half of the 21st century by adding the high-vent, split cuffs and double collar so favored by Japanese senior executives. The suit's material is firm without appearing stiff, and holds a knife-edge crease as well as it stops up to 9mm caliber rounds.

>>>>>[Like *drek* it'll stop a 9-mil. I speak from experience.]<<<<<
—Lounge Lizard (18:39:50/4-23-53)

>>>>>[Oh yeah? Which end of the gun were you on?]<<<<<
—Bung (23:08:20/4-24-53)

>>>>>[Shaddup, fragface.]<<<<<
—Lounge Lizard (19:03:04/4-28-53)

Top off the tuxedo with a "London Fog" evening cape, a knee-length, over-the-shoulder style clasped with sterling silver at the throat. The classic black wool is lined with burgundy Sateen™ woven together with an invisible layer of Kevlar II.

>>>>>[Oh yes, one simply *mustn't* forget the armored evening cape, perfect for achieving the bulletproof Count Dracula look…]<<<<<
—Bung (23:09:02/4-24-53)

MORTIMER OF LONDON

Those who frequent the United Kingdom have long enjoyed the excellence of Mortimer of London, but the exclusive designer has remained generally unknown to fashion mavens on this continent. Now, for the first time, this prestigious Thames-side fashion house turns its attention to the North American market.

Mortimer's product line this season premieres the "Greatcoat" series of outerwear. These warm, heavy coats—waterproofed, and chemically resistant to Seattle's corrosive "hard rain"—look like 20th-century naval greatcoats. They appear to be made of thick, heavy wool and lined with silk, copying the traditional garments on which they are modeled. However, looks deceive. The outer layer of wool is actually very thin; the thickness and characteristic weight of the coat comes from heavy ballistic fabric. The wearer's spine and kidneys enjoy further protection from light, semi-rigid plates handily concealed by the cut of the coat. Ankle-length, designed for both men and women, and available in hard-to-fit sizes, the Mortimer "Greatcoat" lets anyone cut a stylish figure.

>>>>>["Hard-to-fit sizes," of course, means that you can get the coat in extra-grotesque (troll) and extra-squat (dwarf).]<<<<<
—Blackstone (10:49:58/4-14-53)

>>>>>[Laugh it up, breeder.]<<<<<
—Grinder (23:45:21/4-18-53)

>>>>>[Ditto.]<<<<<
—Thorin (22:50:56/4-20-53)

>>>>>[If you can acquire one of these, I strongly recommend it. I find it much more stylish, and much warmer, than my previously favored duster, with much the same protection.]<<<<<
—Tallan (14:11:27/4-29-53)
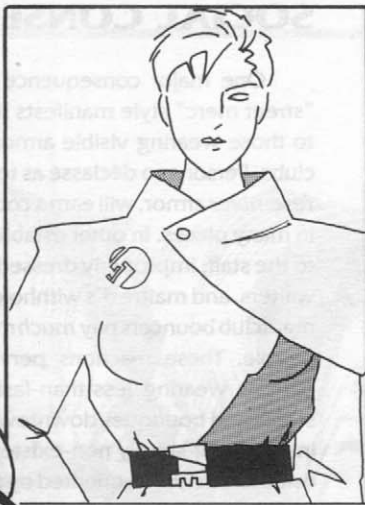
CZARINA ¥7800	
...CTRA ¥4900	
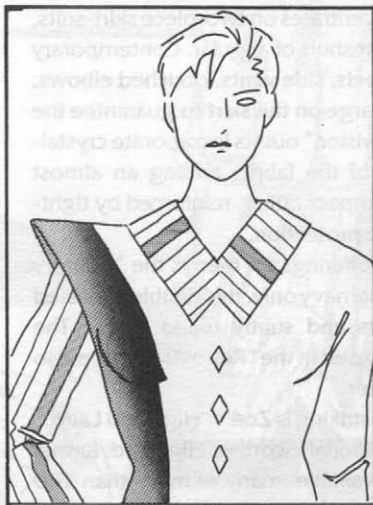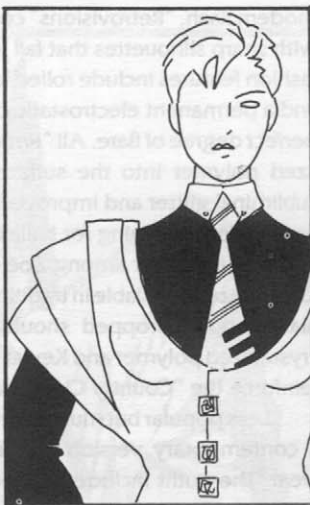
DOMINO ¥10200	VERA ¥4400
NICHT ¥12700	KRISTALLO ¥8100
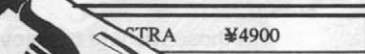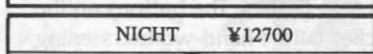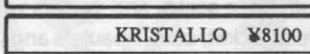
VASHON ISLAND

A local fashion house of growing reputation, Vashon Island specializes in sporty casual wear, bringing back the Old World ambiance of heavy tweeds while infusing them with modern sensibilities and styles.

Vashon Island's "Houndstooth" collection for men comprises a three-piece "country" suit in light tweed, matching woolen slacks with a vest and light tweed sports jacket—all color- and texture-coordinated to create a flexible "mix-and-match" wardrobe. The suit jacket, pants, and slacks feature Kevlar II fibers integrated into the fabric's weave to provide significant ballistic protection. The suit vest and sports jacket lining holds light carbon-ceramic plates, only 1 millimeter thick and custom-shaped to conform perfectly to the contours of the wearer's body.

The "Hunt Ball" collection for women comprises a two-piece skirt-suit with two coordinated pairs of slacks. The jacket and skirt incorporate carbon-ceramic plates for protection, and the slacks are woven with Kevlar II fibers.

>>>>>[Hey, check this drek out: some of these pieces have better impact protection than ballistic armor. Is that possible?]<<<<<
—Banger (13:11:48/2-13-53)

>>>>>[Possible, but not common. I would surmise that the carbon-ceramic plates actually shatter quite easily in the face of the level and concentration of kinetic energy transferred by a slug. I must admit I rather like the layering options these clothes offer.]<<<<<
—Sally (15:59:03/2-21-53)

>>>>>[I got me one of those Houndstooth sports jackets. (Took it off some slag who had no further use for it.) Couple days later I stepped into the line of fire of an Ares Slivergun, and you know, those flechettes went right through the lining of my duster, but the sports jacket stopped them.]<<<<<
—Grond (08:18:21/5-3-53)

>>>>>[Vashon Island also offers a full range of synthleather fashion gloves with a little something extra set into the knuckles and along the edge of the hand: a special formulation of thin macroplast with the density of lead. The macroplast is so thin that it doesn't show, so you can only tell the stuff is there if you pick up the glove—or get slugged with it. Basically, it turns the gloves into a dandy set of knuckledusters. Because the weighting material is macroplast, it doesn't show up on metal detectors. These are vastly overpriced at 350¥ a pair, but you might be able to pick up a pair from a donor who has no further use for them, if you catch my meaning.]<<<<<
—Laura (15:46:46/6-12-53)

ZOÉ

For the last five years, Zoé of New York has produced clothes for an exclusive customer list, designing custom-fitted, one-of-a-kind creations to meet each client's specific requirements and desires. Now Zoé expands into less exclusive, but still limited-edition, lines of clothing.

The newest Zoé creations break away from the design house's tradition of high-fashion evening and ballroom wear and move into cutting-edge corporate fashions. Today's Zoé designs stand out in executive suites and boardrooms throughout North America and elsewhere in the world without looking out of place. And in another break with tradition, Zoé now offers high fashion for men as well as women.

Zoé's most popular new line for women is the "Retrovisions" collection. This "pseudo-retro" style harks back to the corporate fashions of the late 1980s, but imbues them with Zoé's trademark

modern flash. "Retrovisions" concentrates on two-piece skirt-suits, with sharp silhouettes that fall just short of angular. Contemporary fashion features include rolled lapels, side vents, pouched elbows, and a permanent electrostatic charge on the skirt to guarantee the *perfect* degree of flare. All "Retrovision" outfits incorporate crystallized polymer into the surface of the fabric, adding an almost subliminal glitter and improved impact rating, reinforced by tight-weave Kevlar II lining for ballistic protection.

Most popular among Zoé's offerings for men is the "Country Club" blazer. Available in traditional navy only, this double-breasted blazer sports dropped shoulders and subtly rolled lapels. The crystallized polymer and Kevlar II used in the "Retrovision" line also reinforce the "Country Club" blazer.

Less popular but much more striking is Zoé's "Highland Laird," a contemporary version of traditional Scottish Highland formal wear. The outfit includes a kilt available in any of more than 100 authentic clan tartans, a vest, cut-away jacket, evening shirt, neck ruff, knee socks, and garters with side-flashes. The buttons on the vest, jacket, cuffs, epaulets and jacket-tail are hand-worked sterling silver, diamond-shaped and two centimeters across. To complete the outfit, Zoé includes a *skean dhu*, a small, ceremonial dagger worn in the right sock. The somewhat harsh lines of the jacket and vest allow the wearer to incorporate a surprising amount of armor protection, as does the weight and thickness of the kilt.

>>>>>[What guy's going to jander around in a fragging *skirt*?]<<<<<
—Arbeider (12:09:24/3-10-53)

>>>>>[*I* do. And any slag secure enough in his manhood to try it will soon see why. The comfort and practicality are amazing.]<<<<<
—The MacDuff (23:10:32/3-24-53)

>>>>>[So what *do* you wear under a kilt anyway, Mac? Hm?]<<<<<
—Cynthia (14:12:11/3-26-53)

>>>>>[A real lady would never ask. But since it's you, Cyn...on my left thigh I wear a sheathed combat knife; on my right I've got a holstered Predator. Plus I've got my skean dhu, which is actually a monoblade. Hey, Arbeider, if you want to make skirt jokes, *omae*, do it to my face...if you dare.]<<<<<
—The MacDuff (20:14:04/3-27-53)

>>>>>[Okay, so a lot of these products actually offer some reasonable protection. But *frag, omae*, 2K¥ for a man's blazer? Get real...

If you'd rather not pay the big tab and really don't care that much about style, but want something that'll stop heavy rounds, check out Kelmar Technologies' very nice Securetech line of clothing. Not on the cutting edge of fashion, but I kinda like it.

Or if style *is* important, for example, when you need to impersonate a high-level corp suit, look at Ares Arms' Form-Fitting Body Armor. With the "lighter, sometimes diaphanous fabrics, softer silhouettes, and loose, flowing cuts," you can wear some pretty sophisticated protection and it won't show at all.

For info on Securetech and FFBA, check out the *Street Samurai Catalog* that FastJack posted on the board some time back.]<<<<<
—Trasher (18:09:20/4-13-53)

SOCIAL CONSEQUENCES

One major consequence of the movement away from the "street merc" style manifests itself as a change in public response to those wearing visible armor to up-scale bars, restaurants, and clubs. Persons so déclassé as to wear visible armor, or clothing that *resembles* armor, will earn a cool reception or be ignored by patrons in many places. In other establishments, this cool reaction extends to the staff; improperly dressed patrons receive less attention from waiters, and maître d's withhold the best tables. On the other hand, nightclub bouncers pay *much* more attention to improperly dressed people. These reactions pervade all facets of life; prospective patrons wearing less-than-fashionable clothing at the exclusive stores and boutiques downtown can expect brusque, supercilious, insulting, or simply non-existent service. In the true "inner-circle" establishments, frequented by the *crème de la crème*, the management may simply refuse service or entry to those who wear obvious armor.

For those wishing to enjoy the perks of upper-class status, the old saying holds truer than ever, "the clothes mark the measure of the man."

>>>>>[Why did I bother to include this one, you ask? Well, my brothers in the shadows are often forced to mix and mingle with the upper-upper crust, or to impersonate them. Doing this successfully requires knowing their likes and dislikes, characteristics, and mannerisms. Clothing is perhaps the most obvious characteristic of all. If you're supposed to be one of the glitterati and you show up wearing last year's fashions, you won't get too far.]<<<<<
—Captain Chaos (22:57:06/1-7-53)

>>>>>[Even places that aren't really fashion-conscious have started to frown on patrons wearing obvious armor. I've been seeing "No Armor" on the usual "Proper dress required" signs. The bouncers haven't really started to enforce it yet, but it's just a matter of time, I think. Bar, club, and restaurant owners must figure that people are much less likely to start trouble if they're more likely to get hurt—which is definitely the case if you're not wearing armor.]<<<<<
—Zeppo (16:14:15/3-10-53)

>>>>>[What about dermal armor?]<<<<<
—Christian (18:21:58/3-26-53)

>>>>>[Use your head, you zero. If the bouncers don't see it they won't call you on it. (And that holds for weapons, too, by the way.)]<<<<<
—Electric Cruiser (19:36:39/4-28-53)

>>>>>[I've never seen anybody hassled for the basic layer of dermal armor, or even the intermediate. The heavy stuff, however, starts making you look like you've got chitin or something. Dave, chummer o'mine, gets shot at regularly by a bunch of shadow-geek wannabes who think he's a bug or something. Go figure.]<<<<<
—Mangler (05:58:12/5-2-53)

DOC WAGON

ARMED MEDICAL ASSISTANCE
24 HOURS A DAY
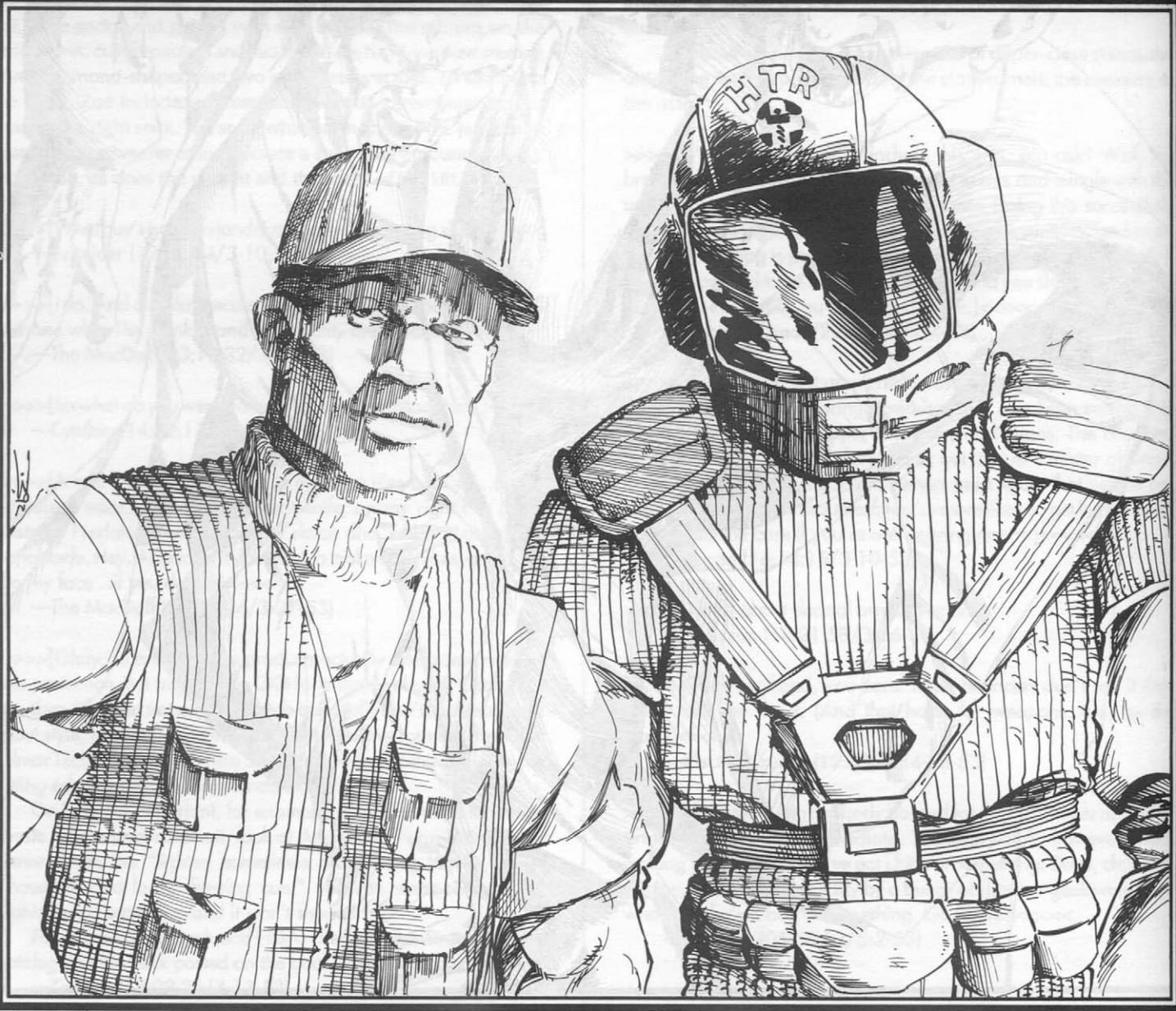
DOCWAGON'S NEW MEDICINE

*E*xcerpted from an editorial letter and response printed in
Asahi Shinbun, January 10, 2053

No doubt exists that Japan possesses the best medical system in the world. The cooperation between health providers and the national infrastructure, the technologies employed, the training of doctors and staff, and the level of patient care all greatly surpass those of any other country. This difference becomes most noticeable when comparing the Japanese health-care system to that of the United Canadian and American States of North America.

>>>>>[I read the original of this piece in the Op-Ed section of *Asahi Shinbun*, a Japanese-only datasheet that enjoys ludicrously high readership among top Jap suits (if you believe *Shinbun's* own readership demographics). The quality of the English translation for *Real Life* came as a surprise: Blakey's software handled the language pretty well. The one thing it blew out on was tone. Japanese communicates subtle scorn and derision like no other language, but the original arrogant, condescending, and anti-anything-that-isn't-Japanese tone got lost in this translation. Anyway, here it is.]<<<<<
—Captain Chaos (13:46:29/1-14-53)

>>>>>[It's not hard to come off better than what we've got in Seattle. I read somewhere, and I believe it, that Seattle hospitals will leave you to bleed to death in the waiting room if your credstick's one nuyen short of the admitting fee—then come after your estate for the cost of cleaning up.]<<<<<
—Hardesty (17:04:14/2-13-53)

It is somewhat galling, therefore, to admit that the UCAS is home to an innovation in health care that has yet to appear in Japan: the private, mobile health-care provider. In Japan, as in many other countries, emergency medical and paramedical service is

provided by the public sector ambulance and emergency-response service, funded directly by the government out of general tax revenue. In the UCAS, however, health care operates almost exclusively for profit. While this situation leads to high health-insurance premiums and massive service and availability inequities, the potential for significant profit has lured a number of innovative companies to enter market niches not directly addressed by public-service health care. The company known as DocWagon™, the first of these providers to begin operations in North America, remains the best known.

>>>>>[…Or most notorious, depending on your point of view.]<<<<<
—Hardesty (17:05:58/2-13-53)

HISTORY

Founded in Atlanta in 2037, the original DocWagon™ organization promised to provide better emergency on-site medical care by responding to calls much faster than any other private paramedical service operating at the time. DocWagon competitors in the Atlanta area improved their response time to protect their market share from this challenger, but DocWagon remained one step ahead by offering new and expanded services to complement its apparently unbeatable speed.

The company named its first major innovation "High Threat Response," or HTR. DocWagon vehicles providing this service responded to calls from regions of the city where other paramedical services refused to venture. In order to provide HTR service, DocWagon armored its ambulances and armed the HTR medical teams. Their next service, the famous "DocWagon Response Guarantee," promised that a DocWagon vehicle would respond to any call for medical aid within ten minutes of the call, or would provide immediate on-site care free of charge.

Next, an unprecedented marketing push by DocWagon popularized the concept of "subscribing" for on-site medical coverage. DocWagon offered contracts to clients willing to pay an annual fee for guaranteed and extended service, plus significant discounts on pay-for-service charges. So successful was this marketing scheme that several years later DocWagon chose to respond only to calls from its subscribers. By this time the reputation and service of DocWagon had so far outstripped its competition that this move guaranteed the company's supremacy in the marketing war. If receiving DocWagon's high-quality service meant signing up for a DocWagon contract, then subscribing became the only logical choice. By 2041, DocWagon had become Atlanta's *de facto* official on-site health-care provider.

Up to this point, DocWagon owned no clinics or care facilities. A roving DocWagon team would pick up an injured client, provide first aid or emergency care, then deliver the client to an accredited clinic or hospital. In 2041, however, the DocWagon corporation made a move that further consolidated its hold on the health-care market: it purchased a small for-profit hospital about to go out of business. Using its finely honed management skills, DocWagon soon turned the ailing business around, and the first of several DocWagon Acute Care Clinics in the Atlanta area became one of the corporation's largest profit centers.

In 2042 DocWagon extended its new vision of health care beyond the Atlanta area. In a marketing campaign never duplicated

in intensity, DocWagon began franchising its operation throughout the remaining contiguous UCAS, excepting Seattle. The company carefully considered and coordinated its decision to expand. Though DocWagon's many detractors claimed that the franchises could never uphold the level of quality associated with the original organization and would thus destroy the parent corporation's profitability, these nay-sayers were quickly proved wrong. DocWagon took exceptional care in evaluating the organizations applying for franchises. The franchise cost, calculated to discourage all but the most serious prospects, totaled 7 million nuyen, a stratospheric sum in 2042. DocWagon further ensured quality by including an "override" clause that required the franchisee to pay the parent corporation a percentage of its *gross* income for the first decade of operation. Other restrictions appeared equally stringent, such as the requirement that the franchisee have been in the health-care industry for at least five years, and that the franchisee operate an independent acute care facility. The franchising package carried so many conditions and restrictions that a new group of nay-sayers arose, claiming that no one would accept the franchise contract on those limiting terms.

Again, DocWagon proved them wrong. By the end of 2042, the company had sold at least three franchises in each major UCAS city—again excluding Seattle—and had many more scattered throughout the country's smaller communities. DocWagon canceled the contracts of no fewer than ten franchisees within the first year of operation for defaulting on terms of the agreement. The parent organization immediately resold the contracts to the defaulters' most avid competitors at a significant discount. The other franchisees took this object lesson to heart, and DocWagon has not been forced to repossess a franchise since 2043. The contractees strive to maintain and even enhance the high quality of service and reputation of the original organization.

In 2043 DocWagon went international. Rather than selling their franchises directly to other countries, which would have entailed sorting out a grotesque tangle of legal complications, they created a "secondary franchise" structure. Approaching large corporations in CAS, California Free State, and some of the Native American Nations, DocWagon sold these corporations the right to franchise DocWagon-style operations in those countries. (Legal restrictions prevented these other countries from using the DocWagon name.) No one can confirm the amount of the initial "secondary franchise" fee, but rumor places it in the low billions of nuyen. As with the UCAS expansion, DocWagon added its standard "override" clause to this astronomical sum, demanding a percentage of all sub-franchisees' gross income.

DocWagon finally moved into Seattle in 2043, amidst claims that the organization was forced to relax its rigid requirements somewhat in order to find a Seattle-based organization that could qualify for a franchise. Whether or not this rumor is true, even its sternest detractors must admit that the Seattle-based DocWagon operations measure up admirably to the standards set by their predecessors.

>>>>>[Not all the time, chummer. Some local franchises—specifically one or two in the outlying regions—don't stand by the standard ten-minute guarantee.]<<<<<
—Hardesty (17:31:23/2-13-53)

DOCWAGON CONTRACTS

In order to provide the best possible service to its clients, DocWagon requires all clients to provide a tissue sample to be filed in a secure vault protected by bonded and armed guards. All samples are extensively tissue typed, and the information stored in the client's electronic file. When DocWagon picks up a client, the trauma team on the scene and the acute care clinic to which the client will be taken can access the file immediately. Both teams then determine treatment for the client based on blood type, HLA, and other compatibilities. The tissue sample also serves as a source of genetic material if it becomes necessary to grow clone tissue for replacement.

>>>>>[That's one thing that *really* bothers me about holding a DocWagon contract. How secure is that "secure" vault, and how trustworthy are the bonded guards . . or the whole DocWagon outfit, for that matter? It chills the drek out of me to think of some corp that I've burned getting access to my tissue sample and using it to slam some nasty ritual sending into me.]<<<<<
—Tace (10:42:09/3-19-53)

>>>>>[It's pretty damn secure, Tace, take my word for it. I've tried to penetrate it—I wanted the tissue sample belonging to a corporator whose life I wanted to make interesting—and I came back empty-handed and pretty bloody. About the trustworthiness of DocWagon itself, I'm not competent to judge. But I'd guess that if every man or woman has his or her price, then so does every corporation.]<<<<<
—Jeff (19:44:24/3-26-53)

Each client receives a sealed-band wrist telephone that broadcasts only to DocWagon, designed as a chemical-resistant plastic band approximately 1.5 centimeters wide and slightly more than 1 millimeter thick. The phone fastens onto the client's wrist like a hospital identification band, but is colorless and translucent, making it unobtrusive. To activate the phone, the client must flip back a protective tab with his or her thumbnail and press the small, flat button inside. The cellular circuitry automatically phones the nearest DocWagon franchise office and triggers a locator circuit in the wrist phone. The phone also establishes voice contact between the client and a DocWagon representative, allowing the client to inform DocWagon of the nature of the health emergency.

The phone band is designed to be worn as a permanent accessory. If the band is ruptured, it transmits a special signal to the nearest DocWagon location and triggers the locator in the band. DocWagon policy requires them to respond to a "band rupture" alert as a High Threat Response call; the client (or his estate) must pay for HTR charges whether or not the response level is appropriate.

DocWagon offers four levels of service contracts: Basic, Gold, Platinum, and Super-Platinum.

>>>>>[If you bust your band accidentally, get on the damn phone *right fragging now* and tell DocWagon you made a booboo. Otherwise it's going to cost you big nuyen.]<<<<<
—Russel (17:10:53/3-10-53)

BASIC SERVICE

Basic DocWagon service operates on a straight pay-per-service basis. The client (or his estate) is liable for the full cost of every service provided by DocWagon except for standard response which is covered by the 5,000¥ annual fee. The following table provides some representative extra-service charges. (*Asahi Shinbun* accepts no responsibility for inaccuracies or changes in these figures. They are included only to illustrate typical costs.)

DOCWAGON™ SERVICE COSTS TABLE	
High Threat Response*	5,000¥
Employee Death Benefit	20,000¥
On-site Resuscitation	8,000¥
Acute Care**	
Basic	500¥/day
Intensive Care	1,000¥/day
Extended Care (3+ weeks)	2,500¥/week

*This is the base charge. The client is liable for any extra expenses accrued during the response call. These include, but are not limited to, ammunition expended, damage sustained by DocWagon equipment and vehicles, health-care costs for injured employees, health-care costs and/or death benefits for innocent civilians killed during the pick-up.

**These figures do not include additional costs for specific medical procedures.

>>>>>[Even with a DocWagon contract, it's expensive to get hurt in Seattle.]<<<<<
—Ronin (11:13:40/4-12-53)

>>>>>[It's a lot *more* expensive *without* coverage. Believe it. Why scrimp on health care if it means you croak in the end?]<<<<<
—Simmons (15:50:49/4-20-53)

GOLD SERVICE

The next level of service includes some significant discounts. A Gold client receives one free resuscitation per year, plus a 10 percent discount on both acute and extended care. Further, the base cost for HTR is reduced to 2,500¥ from 5,000¥. (Additional costs associated with HTR—expenses, death compensation, and so on—remain the same.) Gold contract service is available for an annual fee of 25,000¥.

PLATINUM SERVICE

Platinum service, available at 50,000¥ per year, provides deeper discounts. Platinum service clients receive free HTR service and must pay only death compensation for employees and innocent victims. The client receives four free resuscitations per year, and enjoys a 50 percent discount on acute and extended care. Some DocWagon franchises extend a discount to Platinum-service clients on cyberware implanted as a result of injury, but this is rare.

SUPER-PLATINUM SERVICE

Basic, Gold, and Platinum service are widely advertised. Super-Platinum service, the top of the DocWagon line, is available only to those who know to ask for it.

>>>>>[Probably because it's not cost-effective. The additional benefits aren't worth the additional cost.]<<<<<
—The Keynesian Kid (14:22:52/3-19-53)

>>>>>[Why do people take it, then?]<<<<<
—Nextstep (18:34:58/3-21-53)

>>>>>[Probably just because it's exclusive. Super-Platinum clients are generally your top-rank corporators who'll pick something up *just because* it's expensive. (The company pays for it anyway, so what do they care?)]<<<<<
—The Keynesian Kid (11:21:17/3-30-53)

For an annual fee of 100,000¥ per year, Super-Platinum offers the same discount structure as Platinum service, but the client does not pay for DocWagon employee death benefits. The Super-Platinum client also receives five free resuscitations per year.

>>>>>[If you're getting geeked five times per year, maybe you're not competent to go out on the street, *neh*?]<<<<<
—Webster (23:39:40/2-1-53)

One major additional benefit provided by a Super-Platinum contract is that a Super-Platinum wrist band carries a life-signs monitor in addition to the locator signal and phone. If the client's life signs stray beyond "safe" parameters as defined by the client's race, age, and base physical condition, the monitor automatically places an emergency call to the nearest DocWagon location, triggers the locator

beacon, and, if warranted by the severity of the condition, triggers an audible alarm to help the trauma team locate the client. When the life-sign monitor triggers an alert, DocWagon sends an HTR team unless the client immediately informs the DocWagon dispatcher otherwise.

>>>>>[The DocWagon dispatcher checks all "wave-off" calls with a voice analyzer just to make sure it *is* the client calling in.]<<<<<
—Electron Pusher (01:34:11/2-15-53)

CALLING FOR AID

The easiest and most common method of calling for DocWagon service is, of course, for the client to use his or her own wristband telephone. This guarantees instant communication with the nearest DocWagon franchise, regardless of the client's location. Unusual circumstances, however, can make using the wristband phone impractical or impossible.

In Seattle, at least, and probably elsewhere, DocWagon is connected to the 911 emergency response telephone system. A client can simply dial 911 on any telecom, respond appropriately to the voice prompt, and reach a DocWagon dispatcher. Before a team responds to a call made through 911, the caller must provide either a DocWagon client's Personal Identification Number (PIN) or the serial number printed on a client's wristband. If the caller is unable to supply either number, DocWagon dismisses the call as a prank. If the caller provides the PIN, the dispatcher compares the voice of the caller to the voice record of the client to whom that PIN has been assigned. Upon a successful match, the caller can specify the appropriate type of response and will only be billed for the services requested. If the voice does not match, or if the caller provides only the serial number, DocWagon responds with HTR service and assesses the standard HTR charges to the client whose serial number or PIN was used.

>>>>>[All this rigmarole is to prevent crank calls from tying up the system.]<<<<<
—Barkley (12:08:37/3-29-53)

>>>>>[Crank calls or worse. Remember a couple of years back when a thrill-gang kept calling the DocWagon HTR team just to try and chew them up, for laughs? Charming.]<<<<<
—Street Ghost (13:20:34/4-5-51)

>>>>>[It wasn't just for laughs. Do you have any idea how much a Stallion full of high-tech medical gear is worth on the shadow market?]<<<<<
—The Keynesian Kid (18:21:08/4-10-53)

>>>>>[And the moral of the story is: don't tell *anyone* you don't trust your DocWagon PIN, or let anyone see the serial number printed on your wristband. If they use your numbers to make a call, *you're* going to get charged for it.]<<<<<
—Watcher (10:12:38/4-11-53)

>>>>>[In some regions, DocWagon's hooked up to the PANICBUTTON system. That's not common, though, because then it's tough to know who to charge!]<<<<<
—Guenevere (08:15:11/5-7-53)

DOCWAGON RESPONSE

In most areas covered by DocWagon service, clients can depend on a ten-minute response to a verified call. If the team arrives late, they provide immediate on-site care free of charge.

>>>>>[Uh-huh. Read the fine print, chummers. After you take all the clauses into account, Basic service really only promises response within ten minutes under *ideal* circumstances. Too much traffic? Too bad. As you ascend the contract scale, things get a little better. Only Platinum and Super-Plat unequivocally promise to arrive within ten minutes, but even that service requires the client to be within that DocWagon franchise's immediate response area. If you got your contract through one franchise, and experience problems within the response area of another franchise, the ten-minute response doesn't necessarily hold (though it usually does). If you happen to be outside any franchise response area, only a Platinum or better contract will get you service, and that without response-time guarantees. Once you leave the DocWagon immediate service area, all bets are off.]<<<<<
—Timer (12:31:43/5-2-53)

DocWagon creates a well-defined distinction between three types of calls, each of which requires the service of a specific type of team. The three types of response are Standard Response, Crisis Response, and High Threat Response (HTR).

STANDARD RESPONSE

Basic DocWagon service applies if the client suffered injury or took ill in a relatively safe environment. The environment may pose a threat to the client, and even to the responding team, but no hostile action is taking place. For example, DocWagon Standard Response Teams (SRTs) commonly respond to the scenes of "minor" motor vehicle accidents. These teams carry equipment and personnel similar to the standard public-service paramedic and ambulance services familiar to *Asahi Shinbun* readers. The truck is lightly armored, and the team members carry only small personal arms for protection.

An SRT includes the personnel and equipment required to treat and release victims of minor accidents or injuries. In more serious cases, this team stabilizes the victim on-site, then transports him or her to a DocWagon clinic for additional care.

Not equipped to deal with either large-scale disasters or high-threat environments, SRT teams in the former situation provide what immediate care they can and call in support from one or more Crisis Response Teams. In an environment with high active threat, however, DocWagon standard operating procedure (SOP) authorizes an SRT to attempt service, but nothing more. The team leader decides how to handle the situation, and usually calls in an HTR.

>>>>>[In other words, if the SRT coming in on your call suddenly finds itself under fire, the team is fully authorized to pull out and hide behind something bulletproof. The team leader decides when a situation is "unserviceable" and may pull the team out. The firearms they carry are for dealing with threats to themselves or their equipment, not for assisting the customer.]<<<<<
—Bazingo (06:17:27/4-10-53)

>>>>>[They may be authorized to pull out, but it's surprising how many SRT personnel put their own lives at risk to do what they can on a high-threat call. DocWagon management may care more about the bottom line than about their clients, but the actual personnel are often dedicated as all get-out. Back in 2050, I saw a DocWagon SRT doc wade into the middle of a gang war to pull out a civilian who'd gone down. She took a couple of rounds herself in the process, but she *did* lift the client out. I was impressed.]<<<<<
—Hardesty (16:30:08/4-17-53)

>>>>>[That's a rarity, and she probably got reprimanded for her efforts. DocWagon feels that if you want threat coverage, you should pay for threat coverage.]<<<<<
—Fargo (21:49:35/4-25-53)

Standard Response Teams patrol an assigned region, following a pseudo-random path designated by the ambulance's onboard computer.

>>>>>[This way, they avoid falling into ambushes laid by thrill-gangs on dark nights.]<<<<<
—Norma (10:39:41/3-19-53)

A typical SRT comprises four paramedics, at least one equipped with a datajack to drive the ambulance. SRTs usually use lightly-armored, modified petrochem-powered ambulances. A small percentage of the teams use unarmored versions of the familiar Hughes WK-2 Stallion helicopter. An SRT vehicle contains standard medical equipment, including a defibrillator and emergency surgery gear.

>>>>>[I don't have any facts, but I've heard rumors that these babies pack a drek-hot computer system, complete with a diagnostic expert system.]<<<<<
—Hardesty (10:10:19/2-14-53)

>>>>>[The system exists, but it's still experimental. The way I hear it, it frags the patient as often as it saves him.]<<<<<
—Electron Pusher (11:25:43/3-23-53)

>>>>>[There's a whole fragging pharmacy aboard, too. Lots of wizzer drugs, with a street value in the thousands of nuyen.]<<<<<
—Trasher (11:28:27/9-20-53)

CRISIS RESPONSE

Crisis Response is perhaps the least talked-about service DocWagon provides. Considering the high proportion of the UCAS and North American population carrying some level of DocWagon coverage, any large-scale incident usually involves too many clients for a single SRT to serve effectively. Incidents requiring a Crisis Response Team (CRT) typically include large, multi-vehicle accidents, fires, earthquakes, gang wars, and so on. If a dispatcher receives multiple calls simultaneously from a single locale, that dispatcher may choose to send a CRT to the scene.

A CRT comprises eight personnel, each with the same training and equipment as the personnel making up a Standard Response Team. This allows DocWagon to reassign personnel between the two

types of team. The main difference between the teams is the vehicle each uses. SRT vehicles carry a maximum of two patients at one time; CRT vehicles can carry up to four patients. Essentially, the CRT uses larger versions of the petrochem-powered ambulances driven by the SRT personnel. Most CRTs also use tilt-wing rotorcraft modeled on the familiar Federated Boeing Commuter airframe. These vehicles carry similar equipment and supplies as SRT vehicles, but in greater quantities.

Unlike Standard Response Teams, CRTs do not patrol; they remain stationed at DocWagon dispatch centers, with their crews on standby to "scramble" at a moment's notice.

>>>>>[Watching a bunch of DocWagon people responding to a crisis "Code Blue" is quite a thrill: just like war simsenses of fighter pilots scrambling.]<<<<<
    —Bladerunner (19:01:20/6-12-53)

>>>>>[What isn't so much of a thrill is watching them respond to a crisis like a major fire, piling in and lifting out only DocWagon clients, and leaving the rest to croak.]<<<<<
    —Splattermeister (16:00:20/6-16-53)

>>>>>[That isn't fair. Same as with the SRT personnel, the CRT people are usually dedicated as all hell and very much into the Hippocratic oath. Even if it doesn't put any nuyen into the corporate accounts, most will care for anyone who needs it, and frag SOP.]<<<<<
    —Hardesty (07:21:14/7-2-53)

HIGH THREAT RESPONSE

In North American cities, a distressingly high percentage of calls to DocWagon require a "high active threat" response: both the client and the incoming team face a serious threat posed by the hostile actions of others.

>>>>>[Oh yeah, and that *never* happens in good old downtown Tokyo. Yeah, right.]<<<<<
    —Ronin (13:32:07/2-19-53)

>>>>>[Never.]<<<<<
    —Akira (20:09:31/3-15-53)

Specially trained and equipped High Threat Response teams answer these calls. HTR teams are made up of seven members who fall into two distinct categories of training. Three medical personnel, trained and equipped in much the same way as the personnel who make up SRTs and CRTs, provide medical care to the client.

The other four members of the HTR team function as "threat support personnel." This group protects the medical team and the client from hostile action during the pickup. Though all DocWagon personnel receive medical training, threat support personnel receive a majority of their training and experience in combat.

>>>>>[Watch out for the "threat support" guys, cobbers. They are cranked up, slicked down, locked and loaded, out on the pointy end, and ready to rock 'n' roll *big time*. Most are cybered to one degree or another, and they pack *major* ordnance.]<<<<<
    —Blacknight (16:17:19/2-10-53)

>>>>>[I've heard some nasty tales about threat support personnel, including rumors that some of these guys don't carry as much cyberware as their compadres but are fragging *physical adepts*. If this is true, they're death on two legs in melee combat.]<<<<<
    —Rasta (12:12:32/2-28-53)

>>>>>[Chummers, the HTR team is not there to eliminate your particular problem or bail your butt out of trouble. They show up on-site to pull their customer out and treat him or her. *That's it.* They'll use their weaponry to perform that duty, and for no other reason. They'll fire defensively, but if you think you can pop your wristband when the going gets tough and DocWagon'll coming screaming in to mop up for you, you've got another thing comin'.]<<<<<
    —Wagon Watched (15:51:53/3-23-53)

>>>>>[And pulling a stunt like that invalidates your contract now and forever.]<<<<<
    —Shane (06:38:07/4-27-53)

>>>>>[Now, let's think this through, jokers. An HTR team brings a bunch of gunners along in order to chop down anyone who wants to mess with the lift-out. But in many cases, the people doing the messing are also DocWagon clients…

Interesting conflict of interest. It's my sincere belief that the threat support goons have two jobs. First, they protect DocWagon's investment in equipment and personnel. And second? *Business development.* When they make a high-threat pickup, it's in the DocWagon Corp's best interest if the goons create a little mayhem in the process. If they fire blind into a crowd, there's a good chance that some of the people they wound will also be DocWagon clients…which, of course, generates more calls, more teams dispatched, and more HTR income. Makes a nasty kind of sense, doesn't it?]<<<<<
    —Manta (05:19:22/7-10-53)

>>>>>[You're one twisted puppy, Manta…]<<<<<
    —Kingston (18:23:40/7-21-53)

Like SRTs, High Threat Response teams patrol designated areas, but use vastly different vehicles. Roughly half of HTR vehicles are wheeled ground vehicles, the other half helicopters. The ground vehicles are modified Ares Citymaster urban security vehicles, reconfigured to accommodate the required medical equipment. More lightly armored than standard Citymasters to allow improved speed, HTR vehicles retain the roof-top turret and replace the water cannon with a second light machine gun, generally loading both guns with gel rounds.

>>>>>[…But not always.]<<<<<
    —Stinger (06:16:28/3-18-53)

Currently, the DocWagon air fleet throughout UCAS consists almost exclusively of Hughes WK-2 Stallions with improved armor and two hardpoints mounting a variety of weaponry. In many areas of service, however, DocWagon is gradually replacing this fleet with armed and armored versions of the Osprey II.

>>>>>[The Osprey II, for those who don't know the bird, is a tilt-wing baby, a little smaller than the Federated Boeing Commuter. It's lighter, faster, and just as maneuverable.]<<<<<
—Flyboy (13:17:32/2-18-53)

>>>>>[Watch out for these Ospreys, boys and girls. They've got a couple of hardpoints, which usually mount heavy MGs. I also hear they sometimes pack even nastier stuff like assault cannons, or even miniguns. *Not* a good idea to mess with them.]<<<<<
—Banger (19:50:00/4-2-53)

>>>>>[I had a buddy who tried to boost a DocWagon Citymaster while the team was busy making a pickup. I guess he figured the team might have left the key in the ignition. (I don't know what he wanted with a Citymaster, nor do I *want* to know.) Anyway, the thing was locked up tight, and while he was trying to bypass the lock, one of the DocWagon Threat Support goons came back and blew his head off. Cautionary tale.]<<<<<
—Felicia (11:26:42/5-10-53)

DOCWAGON CLINICS

Among the best-equipped and best-staffed health-care providers in North America, DocWagon central clinics almost rival the standard of health care in Japan, though the level of service provided by DocWagon clinics varies widely. Some facilities provide emergency care only. These clinics deal with trauma cases and immediate medical problems, then transfer the patient to other facilities for further treatment. Other clinics can provide intensive and acute care, but cannot provide chronic or long-term care. And some clinics serve every need, including providing cybernetic replacement if required.

>>>>>[How can DocWagon make money if they transfer patients to other hospitals, you ask? They simply get a kickback from the hospital involved. Unless a DocWagon franchise operates a full-blown hospital of its own, it will usually sign a contract with one independent hospital, to which all transfers are made.
If you find yourself in a DocWagon clinic and don't want to be there—for example, your personal physician is working at Harborview—you can request a transfer. But you should expect to pay DocWagon a hefty transfer fee, usually in the hundreds of nuyen.]<<<<<
—Hardesty (10:59:13/9-18-53)

The DocWagon paradigm provides quality service at an excellent value. The Japanese government and economy might benefit from giving a similar system serious consideration.

>>>>>[What about that other company that tried to compete with DocWagon…what was the name?]<<<<<
—Nash (13:05:17/1-15-53)

>>>>>[They called themselves Crashcart. Yeah, they really came on like gangbusters, competing directly with DocWagon and poaching away some of their biggest clients, guys with those 100K¥-per-year Super-Platinum contracts. They seemed to be making serious headway, then they just pulled in their horns. No more advertising, no

more luring away clients. They're supporting their current clients, but apparently have stopped recruiting. In fact, some people are now leaving Crashcart and moving *back* to DocWagon.
Beats me what really happened, but *something* weird went down. Buzz in the shadows said some slag made a run on the outfit that owned Crashcart back in November or December of '52. Then Yamatetsu Seattle acquired Crashcart, and I guess its new owners aren't too concerned about how their new acquisition's doing.]<<<<<
—Barrett (19:29:20/1-29-53)

>>>>>[That "some slag" who made the run was one Dirk Montgomery, an old chummer of mine. He did the quick fade afterward.]<<<<<
—Quincy (23:59:10/2-7-53)

>>>>>[And the Yamatetsu thing has an angle. It wasn't a straight takeover—the way the facts fell out around here, Yamatetsu purged the entire management structure of Crashcart in a corporate bloodletting so thorough that Crashcart employees still call it "Black Monday." A lot of ex-managers found themselves out on the street.
But the truly odd part of the shakedown is that some of the senior faces from Crashcart Medical Services Corp. never surfaced again. Anywhere.]<<<<<
—Agarwal (21:18:31/2-9-53)

>>>>>[An interesting bit of background. Remember the earlier comments about DocWagon replacing Stallions with Ospreys? Crashcart first brought Osprey IIs into the emergency medical service. I guess DocWagon figured it was a good idea.]<<<<<
—Flyboy (13:28:30/2-10-53)

>>>>>[After "Black Monday," DocWagon bought a lot of Crashcart's Ospreys at fire-sale prices.]<<<<<
—Agarwal (22:06:08/2-12-53)
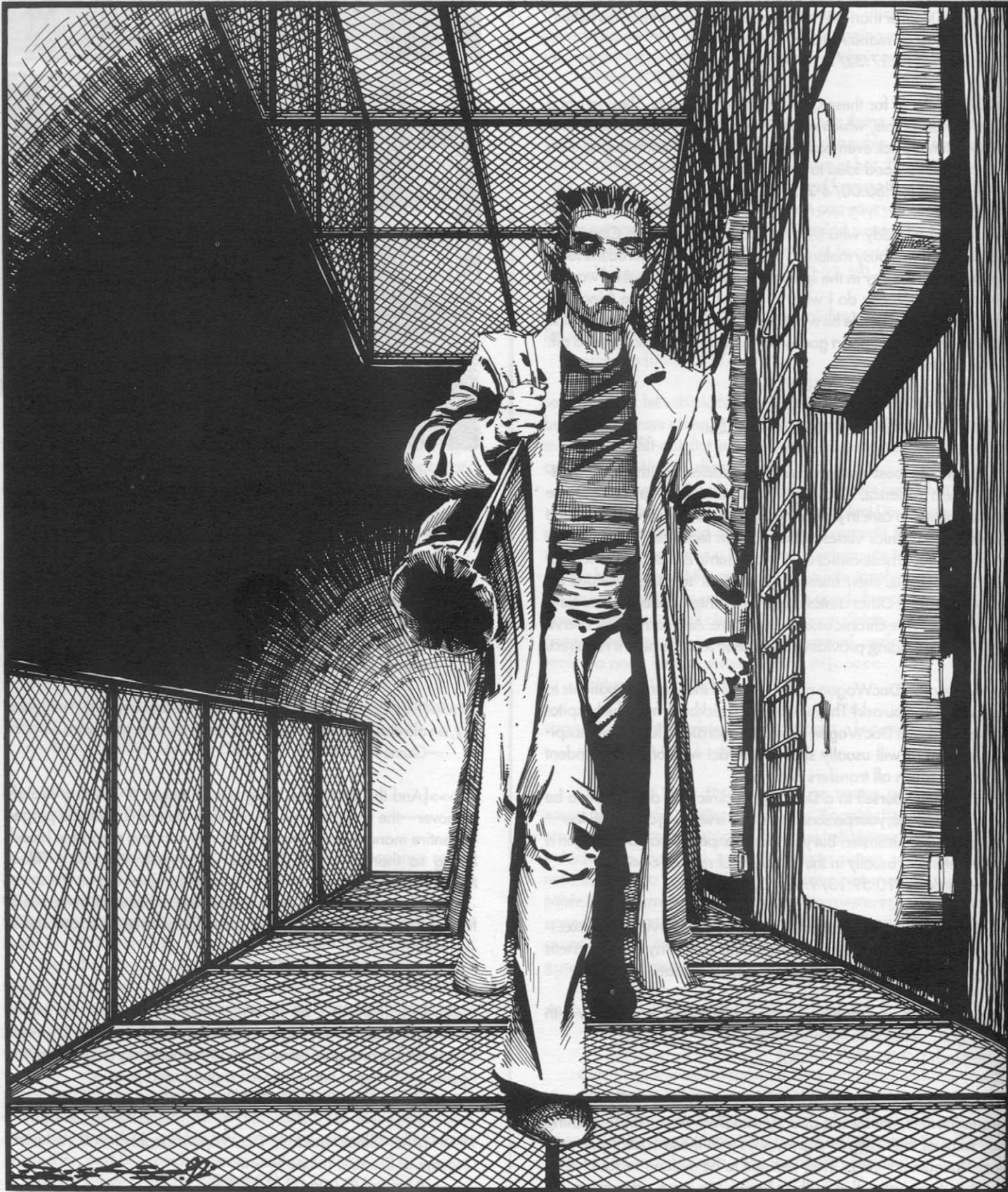
SEATTLE ON 30¥ A NIGHT

*R*eprinted from Westcoast Hospitality, *January 2052*

The first half of the 21st century gave rise to some interesting, though conflicting, trends in the hospitality industry, particularly in metroplexes such as Seattle. The first trend increased service, particularly at hotels and other forms of transient accommodation. Many modern hotels create a luxurious atmosphere that surpasses anything known in the past, offering services and facilities that make the finest hostelries of the previous century look like Spartan shacks. Advanced technology and the increasing use of magic allow guests to enjoy services that previously cost too much to efficiently provide. As amenities increased, so did price. A single suite in a contemporary luxury hotel can easily cost 1,000¥ or more per night.

The second, opposite trend changed the other end of the accommodations scale. At many establishments, guest services have been curtailed or even eliminated to reduce the cost of hostelry. The industry finally admitted that many travelers do not care about lavish surroundings or elaborate guest services. These clients want only a clean, secure place to sleep at a reasonable cost. Some in the industry once believed that such patrons found satisfactory accommodations in rooming houses and "flophouses," and refused to accept that people capable of paying for better services and surroundings would not want to do so. Today, we recognize that ability to pay and willingness to pay are not the same thing.

The Japanese recognized the truth in the final decades of the last century. They realized that many businessmen and other travelers simply needed a bed in a secure place for the night. They intended to do no entertaining in their room; they would eat elsewhere, and so needed no restaurant or room service; apart from the bed, they needed no furniture. Why, the Japanese hostlers asked themselves, should these individuals have to either pay for services and facilities they neither needed nor wanted, or face the indignities of a squalid flophouse? What nature of establishment would best fulfill their needs—nothing more, nothing less—at a reasonable price?

HISTORY AND DEVELOPMENT

The answer became the "coffin hotel." In these establishments, a "room" consisted of a coffin-shaped cubicle, approximately one meter wide by one meter high by two meters long—just large enough to accommodate a bed and to allow the patron to crawl in and secure the door behind him or her. The coffin hotel provided communal sanitary and other facilities, including kitchen facilities, vending machines, and often coin-operated laundry equipment.

Coffin hotels sprung up in many Japanese cities, the largest establishment being the Shinjuku, across the road from Shinjuku Station in Tokyo. By 2005, this hostelry boasted an astonishing *350* cubicles! The most frequent patrons of coffin hotels were businessmen forced by missed trains or other scheduling problems to stay overnight at train stations and airports.

>>>>>[They were also a big hit with sararimen who got too blasted to make it onto the train home after an evening of heavy drinking.]<<<<<
    —Ryoki (14:17:16/1-30-53)

Around 2010 coffin hotels crossed the Pacific and began appearing in North America. Initially much smaller than their Japanese counterparts, these early establishments used the same basic design and locations, in or around airports or bullet-train stations. Coffin hotels took much longer to catch on in North America. Many people found the small cubicles claustrophobic, and the whole concept dehumanizing. But the fact of their efficiency and convenience when other accommodation was unavailable remained.

These early North American establishments frequently offered more "peripheral" services than their Japanese counterparts. While the cubicles themselves provided much the same facilities, the buildings housing them often included restaurants, bars, and coffee shops, plus laundry and other services.

Until about 2035, most coffin hotels throughout the world maintained a front desk similar to that in a standard hotel, with at least one clerk on duty around the clock. This added significantly to the hotel's overhead—and thus to the cost of a cubicle—but automation remained too unreliable to represent a viable alternative.

By 2042 this situation had begun to change. Many establishments began to replace the human element with electronics, and while automation required considerable initial investment, day-to-day operating costs dropped significantly, making fully-automated operation an attractive alternative. Today, of course, coffin hotels in which guests have absolutely no contact with (meta)human employees throughout their entire stay are common.

COFFIN MOTEL

1 meter

1. 'Coffin'
2. Staircase
3. Washrooms & Showers
4. Catwalk
5. Hallway
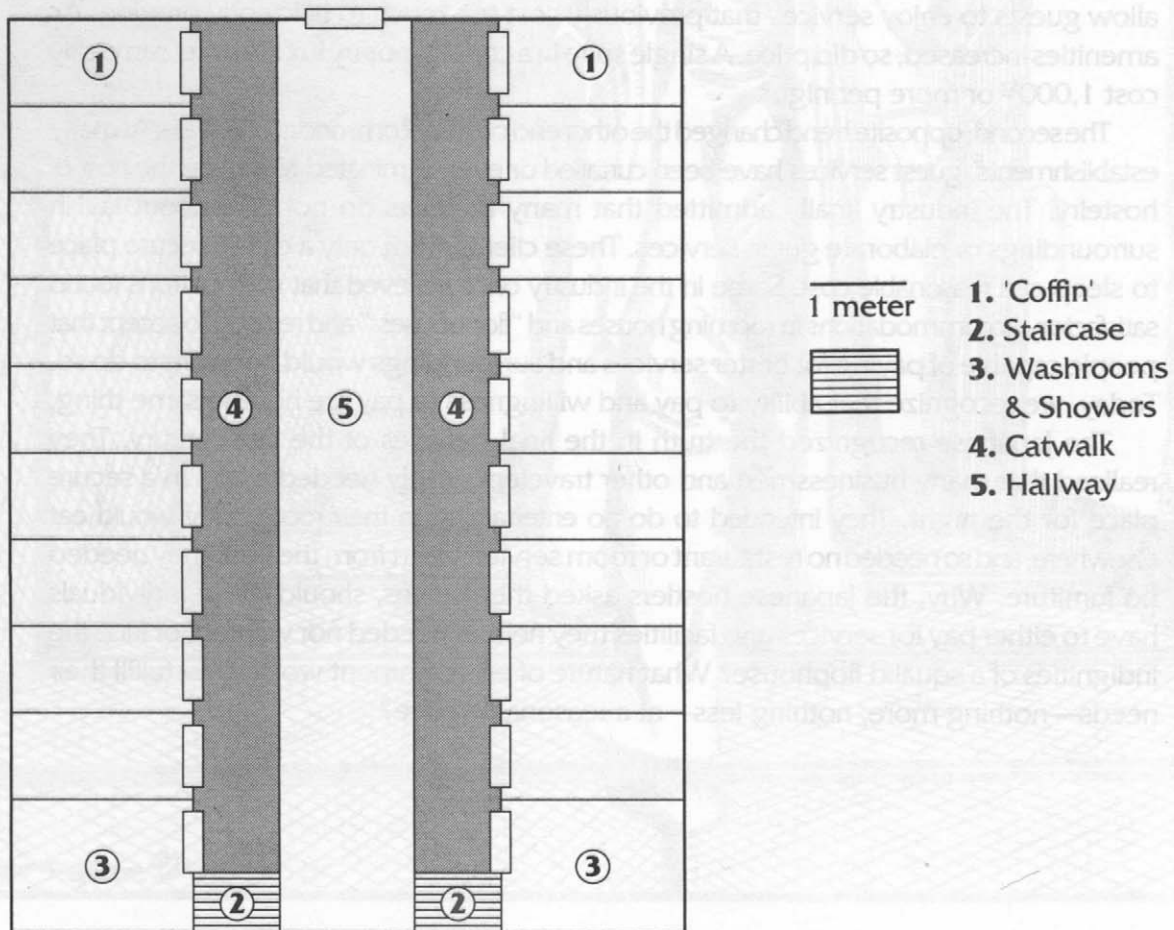
During this same period, coffin hotels began to spring up in locations other than the traditional ones near transit stations. Their undeniable efficiency in using limited floorspace made it only a matter of time before developers recognized their potential. A building too small to provide more than six or eight standard hotel rooms easily housed 40 or more "coffins." And research proved that individuals other than business travelers appreciated the option of extremely low-cost, no-frills temporary housing.

>>>>>[In other words, the developers finally recognized the significant market represented by the city's underclasses who just couldn't afford anything more pricey than a coffin for the night. Disturbing as it may be, many people *live* in coffin hotels on a long-term basis.]<<<<<
—The Keynesian Kid (02:30:43/2-19-53)

STANDARD COFFIN HOTEL

The most common style of coffin hotel in downtown Seattle consists of a building in which the interior walls are replaced by racks of coffins stacked one on top of another to look much like safety deposit boxes in bank vaults. Racks can be prefabricated elsewhere, then simply installed on-site. Many hotels are constructed to allow additional racks to be added later.

A standard coffin rack holds six to twelve cubicles on each of four or five levels. Patrons reach individual coffins in levels above the ground by climbing steep stairs or ladders, then walking along metal catwalks to reach the appropriate cubicle. The catwalk provides only enough space for a client to crawl into his cubicle. The coffins themselves consist of standardized tubes of reinforced construction plastic mounted in metal or concrete-composite frames.

Most hotels offer one communal toilet and shower room at the end of each level of cubicles. Some buildings offer additional sanitary facilities on the ground floor or in an adjoining building.

STANDARD COFFIN CUBICLE

Each cubicle contains only the bare necessities. In addition to a bed with a thin mattress and bedclothes, a cubicle usually offers one or more small, swiveling reading lights mounted in the ceiling. The "head" end of the cubicle, opposite the door, stores a limited-function telecom, a flat-screen trideo, a digital clock with alarm, controls for the cubicle's independent heating and air conditioning, and, in some establishments, a limited-function simsense player. Customers may purchase these additional facilities on a pay-per-service basis. To activate any of these amenities the occupant must insert a credstick into the cubicle's electronics slot.

>>>>>[Rates for these additional services range from minimal to outrageous. For example, to place a local call, expect to pay anywhere from 1¥ to 5¥. Trid service usually runs in the 5¥/hour range, while simsense service often costs twice or three times that price. Other computing services, if they're even offered, get pricey as hell. Many of the phones are dial-out only, and won't even accept incoming calls. If you're expecting an incoming call, use your cellular.]<<<<<
—The Keynesian Kid (02:41:01/2-19-53)

>>>>>[If any of you out there think you can prance into a coffin hotel and clean out all the telecoms or trideos or phones or whatever, think again. The people who build these hotels know people like you are out there, and go to considerable lengths to slot you up.

Sure, every coffin in the place has its own trid. But the unit mounted in the cubicle isn't the whole trideo. Most of the "smarts" of the unit are built into the building's computer system, and, predictably, that computer system is very well protected, thank you. Sure, you can rip the screen out of the cubicle, but it won't work on its own, and isn't worth much as spare parts.]<<<<<
—Ao (15:01:15/3-23-53)

>>>>>[Furthermore, many of these vile establishments mount video cameras in the electronics space to record the image of anyone tempted to engage in petty vandalism.]<<<<<
—Tal Gilgalad (19:26:13/3-25-53)

INDIVIDUAL COFFIN
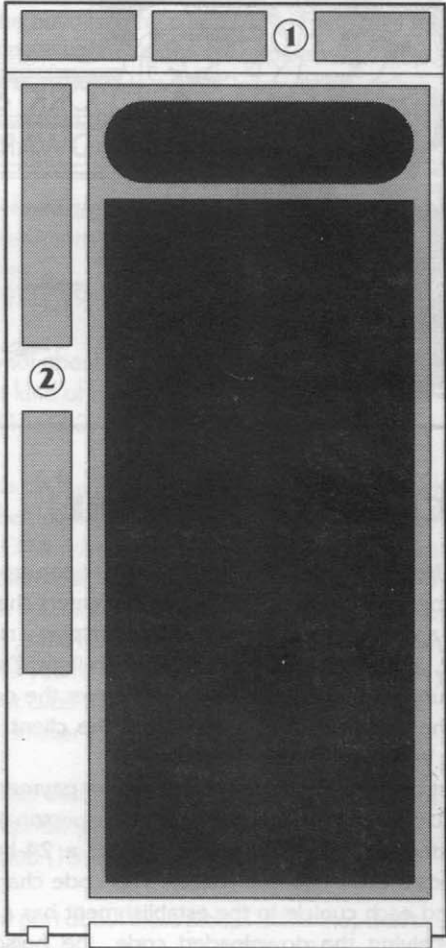
1/2 meter

1. Electronics space
(trideo, phone, light controls, etc.)
2. Storage space, clothes hooks, etc.

CHECK-IN PROCEDURE

The front door of a coffin hotel remains open around the clock. A customer looking for a cubicle simply enters the building and looks for a vacant space. Rented cubicles display a red light beside the door, available cubicles show a green light. The doors of all vacant cubicles lock automatically whenever the door closes. To unlock the door and rent the cubicle, the client must insert a credstick in the slot beside the door.

Most coffin hotels offer two options for payment: personal or certified credsticks. When a patron inserts a personal credstick, the system deducts the appropriate cost for a 24-hour stay, and downloads a code to the credstick. This code changes every 24 hours, and each cubicle in the establishment has a unique code. Upon receiving the downloaded code, the personal credstick becomes the "key" to open the door lock. To enter the cubicle any time within the 24-hour period paid for, the client simply inserts his or her credstick in the slot.

Those patrons who prefer may use a certified, rather than personal, credstick. In this case, the client inserts a certified credstick into the slot, then presses his thumb against a scanner set into the

wall beside the door. The computer system deducts the appropriate charge from the credstick and records the client's thumbprint. For the next 24 hours, that thumbprint unlocks the door.

At the end of the 24 hours, unless the client specifically requests a longer-term rental, the lock code for the door changes, and the system purges the thumbprint data. If the client wants to open the door again after his or her 24 hours has elapsed, he or she must purchase another 24 hours of access.

>>>>>[This code change happens whether you're outside the coffin when the 24 hours is up or *inside* it. In other words, if you stay inside the coffin past "check-out time," the system locks the door with a new passcode and you can't get out. To open the door again, you've got to slot your stick into the socket on the inside of the coffin, and be charged for another 24 hours.

Some places operate on a sliding scale and allow clients a grace period. For example, if you missed check-out time by less than one hour, say you've overslept, you can pay a diminished charge—sometimes as low as a 10¥ "late fee"—to get out. That's not a universal policy, however, so make sure you're paying attention.]<<<<<
        —Molly (11:13:00/4-21-53)

>>>>>[What happens if you're locked in and you don't have the credit to get out again?]<<<<<
—Misfit (13:15:46/4-23-53)

>>>>>[Use the autodial on the phone to call the manager. He'll arrive (eventually), usually with a security guard along, to let you out…but only *after* you've made suitable arrangements for payment.]<<<<<
—Robson (15:01:07/5-1-53)

>>>>>[The door locks behind you every time you enter or leave the coffin. As long as your account's up to date, you can open it from the inside just by pushing a button. That means you *can* open up and let someone else in if you want to—a cube doesn't have enough space for *real* entertaining.]<<<<<
—Lace (21:28:15/5-4-53)

>>>>>[Wanna bet?]<<<<<
—Haetera (00:11:41/5-6-53)

>>>>>[Letting someone in *isn't* generally a good idea. Most coffins don't have viewers to let you see who's knocking.]<<<<<
—Hangfire (15:29:20/5-10-53)

>>>>>[Can you jam the door open?]<<<<<
—One-Ball (23:51:55/5-12-53)

>>>>>[I knew someone would ask that. Yes, you can, the door motor isn't very powerful. But, as soon as you jam the door, the system calls the manager and security. The door stays open for no more than 10 seconds, whether you open it from the inside or outside, unless you hit the button to close it sooner.]<<<<<
—Molly (12:06:44/5-13-53)

SECURITY

Sophisticated, computer-controlled locks secure the doors of coffin hotel cubicles. Those locks and the associated credstick-reading circuitry ensure that only paying clients use the cubicles. A central computer monitors the status of all the locks. Constant updates allow the building management to ascertain at any given time which, and how many, cubicles are in use, and to check for problems. The computer system may be located anywhere in the building or even outside it, using the Matrix for communication, but the system is always secure.

>>>>>[I've got a nasty feeling the system does more than run the locks and count the nuyen. It also probably keeps track of everyone who's ever used the hotel and when, using personal credstick information as a record. Most of that data's going to be trash, but it could be useful for blackmail. And maybe I'm paranoid, but I'm convinced the thumbprint scanners *don't* dump the data when the rental period expires. I'm willing to bet the system keeps the data on file, and so if you've got the right connections, you can get a positive ident from a thumbprint…]<<<<<
—Barkley (20:13:10/2-12-53)

>>>>>[You *are* paranoid.]<<<<<
—Illuminatus (23:26:03/2-12-53)

All cubicle locks can be overridden from the central computer. The system operator can also change the lock codes and lock or open doors individually, regardless of the condition of the renter's account.

>>>>>[…or the wishes of the occupant. Heh heh.]<<<<<
—Snake (05:15:03/3-10-53)

>>>>>[Yeah, but the computer system is pretty tough to hack into, *omae*. It's no cake walk no matter how good you are.]<<<<<
—Matrix Runner (11:32:11/5-2-53)

>>>>>[To quote Haetera, wanna bet?]<<<<<
—Retro (03:32:50/5-7-53)

The computer system also monitors the many fire, smoke, and heat detectors located throughout the building. If a fire breaks out anywhere in the building, the computer immediately triggers the sprinklers in that area and calls the fire department. Tampering with the sensors or the sprinkler system in any building is a felony in Seattle. Closed-circuit video cameras, feeding directly to storage, monitor the common areas of the hotel.

>>>>>[These places don't seem too concerned about preventing trouble. They seem more worried about being able to nail the guy who caused it.]<<<<<
—NFA (11:41:29/4-11-53)

>>>>>[Hey, what about maid service, changing the beds, cleaning the rooms, that kind of drek?]<<<<<
—Drifter (15:43:27/4-21-53)

>>>>>[Depends on the hotel. In some, real people swab the vacant cubicles. (Not the kind of job I'd want, considering the kind of drek who live in coffins.) Others don't give out bedclothes and make everything in the coffin waterproof. Any time the cube is vacant—and I kid you not—the system automatically hoses it down with high-pressure anti-septic and water, which drains out through grills in the bottom. Find out whether the hotel you're flopping in uses this system *before* you leave your stuff in your cube when you go out for a bite.]<<<<<
—Happy Hotelier (06:47:36/4-27-53)

>>>>>[Remember that coffin hotels do not provide astral security, and take appropriate precautions.]<<<<<
—Cyber Stud (15:49:00/5-1-53)

>>>>>[The best part about these places is that they don't cost much. In Seattle, expect to pay anywhere from 20¥ to 35¥ for a night.]<<<<<
—Xist (11:40:19/5-27-53)

>>>>>[Also note that most coffin hotels don't offer a high-speed Matrix link for telecommunications. Check around, though. Some do, which should tell you what they're really in business for…]<<<<<
—Walt (12:41:45/5-28-53)

GUARDING THE TILL

***R**eprinted from* **Seattle Business,** *Winter 2051*

Gloria Yu ran a small corner store on G Street SE in Auburn. She had been in business at that location for almost a decade, and area residents knew her well. Her store and the friendly greeting she gave all her customers had become fixtures in the neighborhood. Her customers considered her a friend, and vice versa.

Until the night of June 3rd, 2051.

At just before ten o'clock at night, closing time for Yu's Grocery, Gloria was stocking the counter displays, preparing to log out the cashdesk computer, and generally cleaning up. An ork entered the store.

>>>>>[Before we get underway here, I want to point out that this piece is pure "advertorial." The chika who wrote this article on security systems for small businesses is one Sheila Bailey, owner of Bailey Security Control Systems, one of the sprawl's major purveyors of—you guessed it—security systems for small businesses. I guess that means we can look forward to *really* objective and unbiased reportage, right? Yeah, right.

So why'd I post it? Well, if you ignore the drum-beating and flag-waving and the frequent references to Bailey products, Sheila discusses topics of interest to lots of you street monsters out there. Sure, you've all got your brand, spanking, new autopistols in concealed holsters, and you think you're going to have no problem schlepping all over town with them, right?

Read this article, and rethink that self-satisfied position, buckos. Remember: the stuff Sheila-scag talks about falls within the budgets of many small businesses. Just what kind of wizzer gear do you think the *big* boys like Aztechnology, Renraku, and MCT use, hmm? Makes the blood run cold just to think about it…]<<<<<

—Captain Chaos (23:31:36/1-7-53)
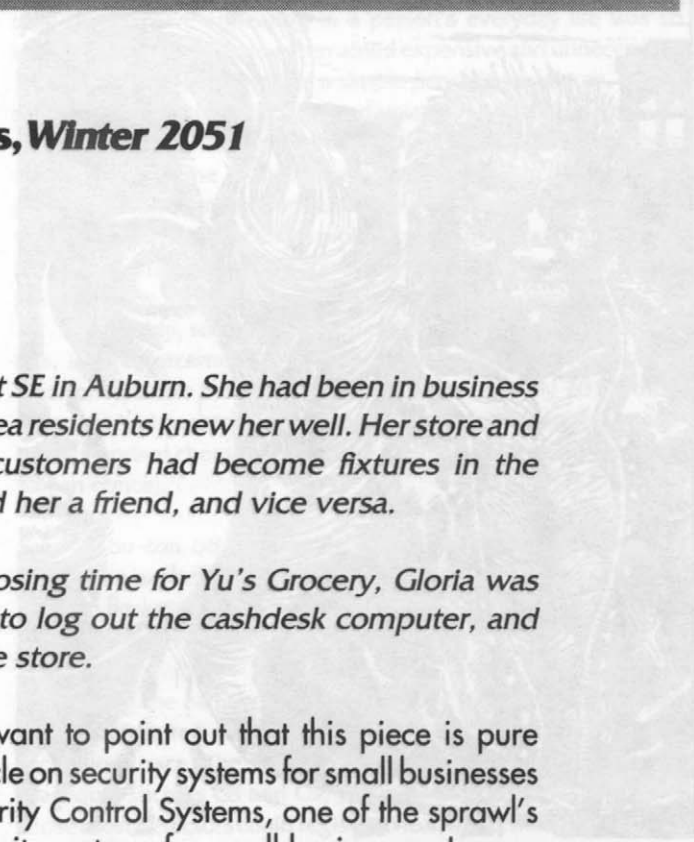
Not one of her regular customers, she saw at once. He appeared hard and cold, dangerous-looking in his black synthleathers. The flinty look in his eyes disturbed Gloria on a deep, subconscious level. But he was a customer, so she greeted him with a smile and a cheery word. He regarded her silently, then moved toward the back of the small store, blocked from view by a rack of stuffers.

Concerned by this break in her routine, Gloria could do little but hope that the ork would buy what he wanted and leave. She tried to watch him in the tiny parabolic mirrors she had mounted at the corners of the room, but could only catch fleeting glimpses of the metahuman. Later, she would remember thinking it seemed almost as if he knew exactly how to avoid the concealed mirrors. She tried to ignore the black-clad figure and the almost palpable sense of menace that surrounded him, and go about her business.

Crash! The sound of something breaking came from the back of the store, near where she'd last seen the ork. Quickly logging off the computer, she hurried to the back.

The ork stood at the back corner of the store, in an area not covered by the parabolic mirrors. At his feet lay a shattered container of pickles. The ork faced her, hands on his hips, his cold eyes fixed on her. A hint of a smile twisted his thin lips.

She heard a sound behind her. Gloria spun. There was no one there. She heard the sound again, and recognized the metallic click from the front of the store as the sound of her front door being locked from the inside. She ran back toward the cash desk and the phone, sick horror twisting in her stomach.

Another click, and the lights went out. Gloria skidded to a stop in the sudden darkness, her labored breathing loud in her ears. Figures moved in the gloom ahead of her, black-clad figures. She shrank back…

And a hand touched her shoulder. With a muffled shriek, she spun. The first ork loomed behind her. She spun again, ready to sprint away. But three more dark figures blocked her path.

The ork smiled, baring yellow fangs. He reached out, and his fingers tightened in her hair. His smile broadened. His breath smelled sour in Gloria's face.

Gloria screamed. And her night of hell began.

>>>>>[Wow, talk about purple prose!]<<<<<
—Webster (20:50:52/2-19-53)

Scenes like this occur with disturbing regularity in the plex. Gloria Yu could have avoided this tragedy by taking appropriate precautions.

STEP ONE: DETECTION

It is an ugly fact of life that Seattle's streets bristle with lethal weapons. Though relatively strict laws against the possession, transport, and use of weapons exist, many parts of the city pay only lip service to enforcing these laws. Many individuals carry unlicensed or even restricted weapons, confident that the police will not trouble them. A recent estimate by an independent research firm states that 72 percent of the pedestrians walking the streets of downtown Seattle on any given day have illegal weapons in their possession.

>>>>>[Hold the phone. This "independent research firm" is actually owned—indirectly, of course—by Bailey Security Control Systems. Take the 72 percent figure with a big grain of salt.]<<<<<
—Tanya (11:27:21/2-18-53)

>>>>>[Yeah, but who cares? Who really gives a drek if Ma and Pa Kettle are packing heat? It's the gangers, chippies, gutterpunks, and assorted street apes we need to worry about, and Tanya, you can bet your sweet behind that they're carrying ordnance.]<<<<<
—Crosshair (12:23:04/3-1-53)

The vast majority of crimes against small businesses fall into the category of armed robbery. Individual criminals or groups of gangers enter a store and hold the proprietor—and any customers unlucky enough to be caught in the situation—at gunpoint while they ransack the establishment. In a frightening number of cases, these crimes end in at least one fatality. Perhaps the proprietor makes a move that the criminal objects to, or perhaps one of the customers recognizes a ganger. The robbers may simply decide that dead men tell no tales, and that live witnesses represent an unwanted complication. Obviously, it is in a small business owner's best interest to determine which "customers" entering their establishments are packing weaponry. Forewarned is forearmed.

WEAPON DETECTORS

The majority of contemporary weapon detectors make use of magnetic anomaly detection (MAD) technology, available since the middle of the 20th century. Technicians mount detection circuitry in the frame of an establishment's front door or build it into an arch distinct from the doorframe. In essence, this circuitry functions like the metal wire coils of an electromagnet, except that the system does not require a current running through it. When a piece of ferrous metal such as a heavy pistol moves through the loop formed by the coils, it induces a current in the coils which the alarm circuitry detects. If the nature of the current (magnitude and other characteristics) matches the given parameters of a weapon, the current triggers the alarm.

This explanation oversimplifies the system, of course. Otherwise, harmless ferrous objects such as steel belt buckles would constantly trigger alarms. To minimize false alarms, the technician also attaches a sophisticated microprocessor package to the system that analyzes the detector signal. The RMAD-13 Magnetic Anomaly Detector™ from Bailey Security Control Systems, for example, incorporates an analysis package so sophisticated and a detector so sensitive that the system can distinguish between a hold-out pistol and a nickel-plated cigarette case of the same mass.

>>>>>[Nothing is that accurate.]<<<<<
—Nacht (12:45:08/1-27-53)

>>>>>[True enough. But the technology has improved unbelievably over the last decades. Hell, I remember my grandmother telling me about how it was when she was a kid. They used metal detectors at airports which were tuned so sensitively that they'd go off if you had spare change (metal coins, for those who remember them) in your pocket. Okay, so no system can distinguish a hold-out from a metal cigarette case. But you won't set them off by the metal toecaps on your boots or the zippers on your synthleathers.]<<<<<
—Black Knight (03:48:12/2-8-53)

>>>>>[In most places, people don't take direct action based on nothing but a MAD reading. They just watch you closer. For this common, low-level response, knowing somebody's carrying a hunk of metal that could be a weapon is plenty accurate enough.]<<<<<
—Roadkill (21:49:42/2-13-53)

>>>>>[So carry a gun made of ceramics or composites. Fichetti's got a few on the market, or you could go with something like the old Glock 17 or Glock 19. Great guns, if you can find them, and those things just don't show up on metal detectors.]<<<<<
—Nash the Slash (15:23:40/2-17-53)

>>>>>[Myth. Urban folklore. I wonder how many people have got themselves geeked for believing that drek?
Even though Glock and Fichetti make their main frame assemblies out of ceramics and crap, the barrels, the chambers, sometimes the slides, and other assorted bits of hardware are metal. If the detector's calibrated right and the analysis software's at all competent, any MAD system will flag a Glock as easily as it does an all-metal beast like a Predator. Sorry, Nash.]<<<<<
—Blaine (23:03:32/3-2-53)

CHEMICAL DETECTORS

Like metal detectors, so-called "chem-sniffers" existed before the end of the last century. Prior to the year 2000, law enforcement used these devices largely for detecting quantities of explosives. The spate of terrorist bombings in the 1970s and 1980s prompted officials to install them at large airports, but the technology was limited to large-scale and government operations. Threat of any type of explosive appearing in a person's everyday life was so minimal that the technology remained expensive and unnecessary.

Chem-sniffers operate on a simple principle. By nature, explosives have a relatively unstable and volatile molecular structure. In other words, they "sweat" certain chemicals into the atmosphere around them. Some of these chemicals, largely nitrogenous compounds, have a distinctive odor; the presence of such an odor signals that an explosive compound is probably close by. Though impossible for (meta)humans to detect, certain animals always react to these scents. In fact, the first chem-sniffers were trained dogs.

Predictably, technology soon outstripped biological capabilities. Law enforcement eventually retired the trained animals in favor of sensitive man-made chemical detectors. By 2010, these detectors had become sufficiently sophisticated to register quantities of standard chemical explosives as small as 10 grams (less than half an ounce).

>>>>>[You can actually get around the process by hermetically sealing the explosives in a container so that the smell can't get out. Vacuum flasks do the job real well.]<<<<<
—Ripper (16:19:49/2-23-53)

During the early years of this century, explosives developers and manufacturers of chem-sniffers engaged in a type of escalating technology race. The chemists developed less volatile types of plastique, such as C8 and C9, that gave off chemicals other than those most detectors could register. Meanwhile, the manufacturers continued to extend the capabilities of their detector systems to include the characteristics of the new explosives. Currently, the manufacturers seem to hold the edge, as no chemical explosive available on today's market can escape detection by the more sophisticated chem-sniffer systems.

>>>>>[Not true. As far as I know, C13 plastique can't be picked up by any chem-sniffer.]<<<<<
—Slax (23:14:51/2-26-53)

>>>>>[True enough. But C13 is a military explosive, and they make sure their toys don't hit the streets. If you can lay your hands on some, I'd be glad to pay you top nuyen for a couple of kilos, but I doubt you can get it.]<<<<<
—Catherine (15:14:26/3-4-53)

In order to extend their technology's use even further, many chemical detector manufacturers added a feature capable of detecting the propellant used in modern, caseless ammunition. A sophisticated detector system such as Bailey's Bloodhound 3000™ can register the amount of propellant in one round of light pistol ammunition. Of course, the Bloodhound 3000 also efficiently

detects every kind of chemical explosive used in grenades, plus standard blasting charges and plastique up to and including state-of-the-art C12.

The effectiveness of any chem-sniffer device degrades as the distance from the detector to the charge increases. For this reason, most contemporary chem-sniffers are built into free-standing archways much like metal detectors. They also fit into standard-size doorframes.

>>>>>[Read this stuff and weep, dudes and dudettes. This kind of drek can ruin your whole day.]<<<<<
—Laker Girl (17:02:54/2-18-53)

>>>>>[Like I said earlier, just keep your explosives in something hermetically sealed.]<<<<<
—Ripper (16:24:49/2-23-53)

>>>>>[Yeah, sure, that'll do it for blasting charges, maybe for grenades. But how do you hermetically seal a fragging *gun*, huh, Einstein?]<<<<<
—Laker Girl (15:05:04/2-24-53)

>>>>>[You can do it, but don't expect to be able to get at the thing quickly.]<<<<<
—Shrimper (23:12:51/3-7-53)

>>>>>[Any technology has a weak spot. Some corps connect their chem-sniffers to their central security computer. Get a drek-hot decker to crack into the system and disconnect the detector, or just suppress the response.

Even stand-alone detectors can be blitzed. A chemist friend of mine concocted a substance that temporarily incapacitates chem-sniffers, kind of the scent equivalent of a flash-dazzle. He turned it into an aerosol, which you can spray into the detector's area. For 10 seconds or so, the thing can't smell its upper lip. On the down side, any sec-guards in the area will probably take considerable notice if you start spraying drek around their detectors.

If you want to buy some of this stuff, call LTG# 206 (31-0113) and leave a message. It'll cost you 7,500¥ for a spray-can good for eight applications.]<<<<<
—Clean Gene (10:17:33/3-13-53)

>>>>>[Yeah, tell me another one. Clean Gene, if you don't know him, would make a great snake oil salesman. Bet he's got a couple of bridges in stock, for sale cheap. I bought some of his "wonder aerosol" and it worked about as well as…words fail me. As you might guess, it didn't work at all, and I almost got my brains blown into my lap.]<<<<<
—Consumer Conscience (17:12:11/3-14-53)

>>>>>[I've tested the stuff and it worked just fine. What's your problem, CC?]<<<<<
—Mouse (05:17:07/3-29-53)

>>>>>[How about some independent arbitration here?]<<<<<
—Laker Girl (18:18:44/4-2-53)

STEP TWO: ALARM

Most systems, including Bailey's RMAD-13, offer several options for alarms. The simplest option triggers an audible alarm, a loud beep or buzz easily heard up to 10 meters away. Some systems offer an accompanying flashing light. Both these options, of course, alert the subject that his or her weapon has been detected. In some circumstances, the knowledge that a weapon has been discovered frequently proves deterrent enough to discourage the bearer from starting trouble.

In other circumstances, leaving a customer or client unsure of whether or not his weapon remains undetected produces more effective results. Did the doorway he or she passed through have a detector, or not? If so, did it register the weapon or not? This very uncertainty can prevent violence in its own way. In such "silent" systems, the detector alarm may be a concealed light, perhaps mounted behind the cashdesk in a small store, or a warning message may appear on a nearby computer screen. For a small additional investment, the system can be configured to sound an audible warning in a "bud"-style earpiece worn by the proprietor.

>>>>>[In larger stores, or in other places with on-site security personnel, detectors alert the sec-guards directly. The Renraku Arcology goes one better; most of their sec-guards have alarm receivers plugged into their datajacks. When the detector picks up a weapon, who, where, even a guess at what is uploaded directly into the sec-guards' brains. I don't know for sure, but I'd guess that the subject who triggered the detector turns up on the visual field of the guards' cybereyes.]<<<<<
—Shane (21:35:05/2-13-53)

>>>>>[Depending on what's going down at the moment, or exactly what the detector protects, sec-guards respond differently. In some places, they'll come over and eject the guy packing the heat, or relieve him of his burden. In other places, they just keep a very close eye on him, ready to drop him in a moment if he makes a wrong move. Sometimes the sec-guards make their surveillance obvious, hoping that knowing they've spotted you will persuade you not to do anything drekheaded. Sometimes, though, they keep a low profile. You won't know they've seen your weapon until you try to draw it. You'll find out you're blown when the first rounds start coming in…]<<<<<
—Sally Shears (21:53:31/2-27-53)

>>>>>[How common is all this drek anyway?]<<<<<
—Solomon Grundy (20:29:57/3-14-53)

>>>>>[Depends on the place. Most major corps have this stuff installed throughout their facilities, and a majority of high-tone restaurants, clubs, and stores carry the latest tech. Even small stores are likely to be on this bandwagon, and I think we'll see more and more of this before we see less.]<<<<<
—Borland (19:27:31/3-28-53)

>>>>>[You want to see a slick system? Check out SeaTac airport, the semiballistic and suborbital departure terminals. *Wow!*]<<<<<
—Flyboy (13:51:31/4-13-53)

STEP THREE: RESPONSE

In many cases, just making security or the proprietor aware that a person has brought a weapon into an establishment is not enough to protect the owner or other patrons. They must also be in a position to do something about it. Of the many appropriate countermeasures available, most fall into two main categories: passive and active.

PASSIVE RESPONSES

A passive response to a detected weapon simply means staying alive while calling for help. This is most easily accomplished by establishing "safe zones" within an establishment such as booths or easily accessible rooms sufficiently armored to stop the standard rounds an intruder might fire. A safe zone should also provide two other features: a locking door too heavy to be forced, and easy access in an emergency. If the layout of the establishment does not lend itself to creating such a haven, the next best option is to armor an obstacle such as the cash desk in a small store, with ballistic composite. While not providing complete coverage, an armored area offers both easy access and partial protection from gunfire.

In the passive response system, once an employee or owner reaches cover, he or she must summon help. A PANICBUTTON or similar crisis-call system built into the safe zone is an obvious choice, but a portable PANICBUTTON transmitter provides a better solution. A small box, approximately 5 x 4 x 2 centimeters, the portable transmitter has a pear-shaped button on its face that triggers all PANICBUTTONs within 20 meters when pressed. The transmitter is small enough to be carried at all times, and can be easily triggered in an emergency. Bailey Security Control Systems markets a PANICBUTTON transmitter under the brand name *OnCall*™ that lists for 500¥. (If she had purchased such a unit, Gloria Yu might have saved herself untold anguish.)

>>>>>[Sheila fails to mention that you've got to hook a receiver into every PANICBUTTON that you want to respond to the transmitter. The receiver, associated circuitry, and installation will set you back another 500¥ or so. (All sold by Bailey, of course.) For 1,000¥ plus, you've got a system to summon Lone Star—but how fast does Lone Star respond to a PANICBUTTON call in the Barrens? Take two shots to the head and call me in the morning.]<<<<<
—Catherine (15:26:26/3-4-53)

ACTIVE RESPONSES

The most common active response of business owners everywhere, and probably the most dangerous, is to reach for a nearby concealed weapon. Though on rare occasion a proprietor may simply produce a weapon and show he is willing to use it and thus scare off intruders, such action usually serves to panic the intruder into violence. Worse, the intruder might decide he or she is being challenged, and respond accordingly. Because small business owners usually possess far inferior skill with weapons than the individuals threatening them, drawing a weapon on an intruder is essentially suicide.

Many other types of active response are available, and none carry the same risk to the user as a firearm. Two of the most popular options appear below.

Netguns

Many establishments in areas rated medium threat by law enforcement standards install net systems in the ceilings. Based on the tried-and-true netgun technology developed by Williams Technologies (formerly Chandler) of New York, the system(s) fire into pre-designated areas where an armed intruder is likely to stand, for example, in front of the cash desk. The net system has no autonomous targeting; the proprietor must wait for the target to walk into the netgun's target zone, then trigger the system, usually with a concealed foot switch. The system fires a net powerful enough to drive a troll to the ground and completely entangle him. The Bailey *Tangler*™ netgun system lists for 1,700¥ (including all associated hardware, not including installation), and most similar systems sell for around the same price.

Gas Delivery Systems

Another nonlethal active response alternative, gas delivery systems flood a considerable area almost instantly with fast-acting narcotic vapor. As with the netgun system, someone must physically trigger the gas dispersion system and the targets must, obviously, stand within its area of effect. Bailey offers an above-average system incorporating standard technology called the *Lethe*™. Each *Lethe* system floods an area up to a volume of 30 cubic meters with fast-acting Neuro-stun IX within 5 seconds or less. (Neuro-stun IX is a quick-oxidizing version of the more familiar N-S VIII and becomes totally inert 5 minutes after contact with oxygen.) A *Lethe* delivery system, including all peripheral hardware (not including installation) lists for 2,500¥. A direct connection to the PANICBUTTON system that will activate the PANICBUTTON as soon as the gas system is triggered, costs an additional 500¥.

>>>>>[Real slick. Fire off some gas inside your store. Maybe the goon with the gun goes down, but so do you.]<<<<<
—Bung (18:03:06/4-11-53)

>>>>>[So what? Better unconscious than dead, particularly if Lone Star's standing around when you wake up. Anyway, who said you have to stay in the area of effect? Gas the fraggers by the door while you duck down behind your armorplast counter, right, Sheila-scag?]<<<<<
—Laser (04:18:18/4-23-53)

Gloria Yu survived her night of torment. Yu's Grocery is still open, out there on G Street SE in Auburn. You'll recognize it. It displays prominent logos on the windows proclaiming, "This establishment secured by Bailey Security Control Systems." Visit her anytime; she'd love to discuss her new security.

But leave your gun at home.

>>>>>[Gets you right *here*, don't it?]<<<<<
—Bart (12:08:18/4-2-53)

>>>>>[Moron.]<<<<<
—Terri (06:09:48/4-7-53)

LAUBENSTEIN·92

EATING FAST AND FEARLESSLY

Reprinted from Seattle Gastronomic, *January 2051*

Normally, *Seattle Gastronomic* would not devote filespace to a fast-food restaurant, but a recent influx of mail has convinced the editors that many readers look for more than quality of food and service when choosing an eating establishment. It is a sad comment on the world in which we live that many Seattle residents consider safety more important than the traditional criteria of quality, presentation, freshness, and service when selecting a restaurant. For those epicures who now rate safety above quality, McHugh's—a fast-food chain native to Seattle and currently limited to the metroplex—proves a wise choice.

LAYOUT

As with many fast-food chains, all McHugh's restaurants are built on a standard layout. Floorplan, facilities, menu, prices, even color scheme do not vary from restaurant to restaurant. Though this symmetry has obvious financial advantages for the parent company, it creates a depressing sense of sameness for the customers. A person sitting in any one McHugh's could be in Kent, Auburn, White City, Everett…anywhere. Even the most discriminating diners admit that these restaurants look crisp, contemporary, and very clean, soulless as they might complain that it seems.

New visitors to McHugh's will look in vain for booths or banquettes. These establishments offer only plain tables constructed of the lightest macroplast, surrounded by chairs made of bent macroplast tubing. (These minimalistic-looking chairs offer much more comfort than their appearance indicates.) Though initially surprising, the choice of the furniture design and material makes perfect sense in view of McHugh's watchword, which is safety.

McHugh's

1. Food preparation area
2. Manager's office
3. Storeroom
4. Women's washroom
5. Men's washroom
● Usual guard position

———————

2 meters

McHugh's management believes that every facet of their establishment discourages people from starting trouble. Their policy of deterrence, discussed in depth later in this article, explains the furniture. Gunmen use booths for cover, and so McHugh's has no booths. The open framework chairs also provide no cover, and the flimsy tables cannot stop even the lightest pistol round. The entire restaurant floor provides perfect sight lines and unobstructed fields of fire for the McHugh's security guards standing sentry around the dining area.

>>>>>[The whole restaurant's a killing ground? What's safe and reassuring about that?]<<<<<
—Tace (13:42:14/1-28-53)

>>>>>[Actually, you're perfectly safe until you start trouble. Then the McCops cut you down. I don't know about you, but the idea of shooting it out with armed and armored sec-guards with nothing but flimsy tables to hide behind doesn't spin my crank.]<<<<<
—Tegger (14:21:51/2-3-53)

Visitors to any McHugh's restaurant will notice with pleasure the large, concrete planters positioned outside the restaurant's front door filled with foliage that adds a bright touch to the building's facade. The planters actually fulfill a different purpose. Each planter measures one meter in diameter by one meter high, and they sit two meters apart. Each one weighs approximately 2,000 kilograms, and is anchored by reinforcing bars to the concrete slab on which the restaurant rests. Large, sturdy, and effectively immovable, these planters provide an effective anti-vehicular barrier.

>>>>>[What is this place afraid of? Car bombs?]<<<<<
—Parrot (13:31:47/2-4-53)

>>>>>[Could be.]<<<<<
—Nora (23:48:27/3-2-53)

FOOD

The food at McHugh's is, to put it bluntly, uninspired. The utterly predictable menu consists of soyshakes, soysundaes, and soykaf to drink, and the food list concentrates on meat-substitute burgers and other such pedestrian fare. The flash-frozen food is stored in autodispensers beneath the counters in the food preparation area. When the customer places an order at the counter, the autodispensers select the appropriate items and route them to the preparation equipment. Cold soykaf gets the microwave treatment, almost instantly reaching drinkable temperature. High-power microwave ovens also defrost frozen soy or krill patties, which then

receive quick surface-broiling under arc discharges to give them an appetizing brown color. Powerful and effective, the equipment can prepare an order for four people in less than two minutes.

And how does it taste? Suffice it to say that McHugh's will never go broke underestimating the tastebuds of the Seattle public.

>>>>>[No flavor, no offense. There's nothing to dislike about it. Nothing to like, either.]<<<<<
—Gourmand (12:11:53/2-16-53)

In its defense, McHugh's fare boasts a high level of consistency. No patron has ever received a badly filled order. Of course, this very consistency contributes to the previously mentioned sense of soullessness.

McHugh's also maintains an exceptional level of cleanliness.

Outstanding hygiene, reasonable prices, and a children's menu make McHugh's a good choice for families. A sample of prices from the menu appear below:

Basic Soyburger   2¥
"The Hugh"—soyburger with processed
    cheese-flavored food   3¥
"The Beast"—triple soyburger with processed cheese-
    flavored food and fried egg substitute   5¥
Soykaf 1¥
Soysundae (13 flavors)   2¥

>>>>>["Processed cheese-flavored food." Gah! What's next? Artificial processed cheese-flavored food substitute?]<<<<<
—Laura (01:59:01/2-13-53)

>>>>>[Check next month's special menu.]<<<<<
—Bung (21:00:21/2-23-53)

SECURITY

Despite its other, perhaps arguable, attractions, many people consider McHugh's high level of security its most appealing feature.

>>>>>[They sure as drek ain't comin' for the food.]<<<<<
—Crusher (14:15:43/2-21-53)

Guards provide the primary source of security, and each restaurant posts six security guards at all times. McHugh's hires its guards based largely on appearance; most of their security force is made up of humans and elves with open, friendly faces and cheerful demeanors. Their well-tailored but casual uniforms fit loosely in order to conceal the fact that they wear armor jackets with reinforced plates protecting vital areas. They carry heavy pistols and tasers in concealed but easy-to-reach holsters and wear black metal-mesh gloves connected to powerful capacitors and battery packs. In addition to armed and unarmed combat training, McHugh's security guards receive intensive courses in interpersonal relations. In accordance with company policy, security personnel react quickly and ruthlessly to the first hint of serious trouble. McHugh's management publicizes this policy widely, well aware that deterrence works only if the deterrent is known.

A sophisticated maglock secures the rear door to every McHugh's restaurant and can only be unlocked by the thumbprint of the manager on duty at the time. The front doors remain closed but unlocked during business hours. Metal and chemical detectors built into the door frame note any customers bringing weapons into the restaurant and relay the pertinent information to the security guards through earpieces. Security guards give polite, but obvious attention to customers who register as carrying a weapon.

When necessary, any security guard on duty can trigger the facility's secondary security system: gas dispensers built into the ventilation shafts. Activating this system automatically locks the front doors and floods the entire restaurant floor area and both washrooms with Neuro-Stun VIII gas within five seconds. A second dispenser system is available to flood the food preparation area, the manager's office, and the storage room with the same gas if necessary.

>>>>>[Gas the customers, huh? That's what I call service…]<<<<<
—Bung (14:38:26/3-11-53)

>>>>>[Like I said in an earlier section, better unconscious than dead, chummer.]<<<<<
—Laser (06:09:54/4-23-53)

>>>>>[Don't joke about McHugh's security, goombah. The McCops are tougher than any other restaurant security, and they're equipped with air filtration bodyware, so gas doesn't phase them.]<<<<<
—Vatjob (14:14:58/5-13-53)

CONCLUSION

Depressing as the thought may be to those who enjoy *good* food, McHugh's remains one of the most successful restaurant chains in the sprawl. Though speed, consistency, and cleanliness play their parts in this success, the main attraction *must* be the chain's high security level. Other establishments, not only fast-food emporiums, but full-service restaurants as well, have taken a leaf from McHugh's book and begun to improve their own security. As long as this effort does not detract from the quality of their food and service, *Seattle Gastronomic* applauds the trend. In the meantime, while safety outranks quality nervous diners can find a McHugh's no more than a couple of minutes' drive from anywhere in the sprawl.

>>>>>[Why the frag would any of *us*—I mean, the non-family types who read Shadowland—want to go to fragging McHugh's?]<<<<<
—Tober (00:02:54/3-17-53)

>>>>>[Believe it or not, it's a great place for a safe, neutral-ground meet. Believe it.]<<<<<
—Dirty Dog (19:01:52/3-29-53)

>>>>>[Besides, where better to arrange a meet with a Johnson who wears a 5,000¥ suit, drives a 50,000¥ car, and whose snippy, fraggin' "classier than thou" attitude twists yer spud so bad you'd like to introduce him to Mssrs. Smith and Wesson?]<<<<<
—Killjoy (17:45:41/4-2-53)

BEST OF HOME SECURITY

Reprinted from Consumer Bulletin, *January 2052*

In any rapidly expanding market, the potential for great financial gain attracts both the qualified service provider and the scam artists to the industry segment. While many newcomers offer genuine goods and services, certain types of companies will depend on lack of sophistication in the marketplace to conceal substandard products and services. As the market matures, companies providing low value lose business to the honest providers, but that market break often comes too late for the unfortunate victims of cons who have paid considerable nuyen for services and products worth less than their cost.

Home security providers offer an excellent current example of a market segment in the pre-maturity phase. For a fee, home security providers promise to deliver services and products designed to protect homes from burglars and other intruders. In the last six months alone, seven new companies entered the home security market in Seattle, bringing the total up to thirteen such providers within the metroplex. Note that these figures refer to "full-service" companies offering a complete security "package." Expanding the parameters of definition to include companies providing only portions of the "security equation," such as specialized alarm companies, locksmiths, consulting engineers specializing in structural "hardening" and others yields more than 100 firms.

Among the thirteen recognized full-service organizations, the quality of service, product, and personnel fluctuates wildly. Wolverine Security, one of the best private security providers anywhere in the world, rivals the excellence of Lone Star, Knight-Errant, and other corporate security specialists. Also-rans such as Jolly Roger Security peddle their trade at the bottom of the scale. Though the industry capably recognizes the difference in reputation between Wolverine and those companies run as scams, the average home owner has few criteria by which to evaluate security companies. Cost, a standard indicator of quality, offers no guideline in this case: Wolverine and Jolly Roger

offer similar rate structures, while Hard Corps Security, one of the top five private security companies, boasts one of the lowest base rates. *Consumer Bulletin* produced the following analysis of the home security industry to provide the layman with a point of reference for determining and fulfilling his property protection needs.

>>>>>[Condemner Bulletin's right about a bunch of things here. Quality range is extreme. Let's look at a couple of the companies licensed to use lethal force: Wolverine, Hard Corps, Bloch Security, and Jolly Roger. Wolverine hires ex-military and ex-Lone Star personnel. You never know if the sec-guard in the Wolverine uniform is actually a multi-tour Desert Wars veteran who's kept up his weapons skills as a hobby since his discharge. Hard Corps screens their applicants almost as thoroughly. Bloch, in contrast, usually hires washed-up ex-cops, wannabes who couldn't hack it in the Star or oldsters who got pensioned off. Competent, but a bit slow. And then there's Jolly Roger. They're licensed to use lethal force, but they're as likely to geek themselves or each other as an intruder.]<<<<<
—Hangfire (11:22:31/2-25-53)

PRIVATE SECURITY TERMINOLOGY

The following definitions explain and clarify the language used by the private security industry to describe products and services.

FULL-SERVICE PROVIDER

The *Consumer Bulletin* defines a full-service provider as a company offering all of the following "base" services: structural hardening, locksmithing, alarm design and installation, alarm monitoring, and mundane patrol. A company unable to provide any one of these elements does not qualify as full-service. In addition to these base services, certain organizations offer biologicals (watchdogs or other animals), astral protection, extended passive defenses (such as electric fences or laser interdiction) and/or active automated defenses (such as autonomously targeted autocannons).

>>>>>[Is this guy drekking me? Autonomously-targeted autocannons?]<<<<<
—Longfellow (13:33:38/2-12-53)

>>>>>[Unfortunately, no. Desert Storm Security specializes in that kind of drek. Of course, the targeting software is just one step above the experimental prototype at this point, so anyone stepping into the free-fire zone risks an even chance that the weapon will either "watch" them without firing, or go into RESET mode and open up. Quite frankly, there's something very scary about seeing a minigun on a hardened pedestal trained out over the rolling lawn of an estate in Madison Park.]<<<<<
—Sue (11:28:00/3-1-53)

ACTIVE AUTOMATED DEFENSES

The technology to create and operate autonomous active defense systems has existed for several years and found wide acceptance in the corporate marketplace. Recently, despite its high cost, this technology has begun to trickle down into the home defense market segment.

>>>>>[I talked about this drek in the corp security file. A couple of estates in the sprawl use this kind of thing. Unlike "intelligent" gun ports in a corp facility, these autonomous gun systems use lethal ordnance, usually light machine guns. "Dumb" gun ports don't work so well outside; randomly hosing down an area with fire doesn't make much sense when the bullets might come down on your neighbor's head.]<<<<<
—The Hammer (23:27:45/12-29-53)

>>>>>[The systems currently available on the open market show a very low comparative accuracy rate. Also, for more reasons than the Hammer stated, many areas have declared autonomous systems to be in violation of the local bylaws. As Hammer said, if a round misses its target, it will end up *somewhere*. In a residential area, chances are that "somewhere" will be somebody else's property.]<<<<<
—Lang (11:33:50/3-1-53)

>>>>>[I got some bad news for you guys. I know for a *fact* that Ares Arms is just about set to market a nasty little system under the Sentry™ brand name: a portable LMG (the top-of-the-line mini-gun) with a full 360 degree traverse mount, about a thousand rounds, and autonomous acquisition and tracking capability. So far, sounds like the same thing everybody else has, right? But wait, it gets better. They link up one of their killer QuickTrac™ tactical computer systems to it, so the fraggin' thing can track up to *twelve* discrete targets simultaneously. Now how much would you pay?]<<<<<
—Hicks (09:15:51/3-12-53)

ALARM DESIGN AND INSTALLATION

Full-service companies always design and install complete alarm systems when hired to protect a home. Almost every home security company, even the lowest quality, can install anything from a simple perimeter system, protecting only doors and windows, to a comprehensive system incorporating motion detectors within that perimeter.

>>>>>[Refer back to the file on Mitsuhama's security system. Any home security company worth the name can install any one of those systems, or a combined system that will make your blood run cold.]<<<<<
—Noël (00:01:32/2-15-53)

>>>>>[Theoretically, yeah. But some systems just ain't right for a home. Remember, people *live* inside. Sure, they might turn on the alarm only when they sleep, but most will get up and go to the can, or grab a glass of water, or whatever. So extensive motion detectors ain't a good idea. Unlike corp facilities, most homes ain't airtight, either, so air pressure systems are out. If the alarm goes off every time the barometer drops, the system's not much good. What you're going to see in a home for security is usually common sense—which ain't all that common, these days.]<<<<<
—Zeeber (15:04:59/3-25-53)

>>>>>[Unless the place stands empty for long periods of time, as does a summer home during the winter.]<<<<<
—Noël (02:06:58/3-28-53)

>>>>>[Uh, yeah, then all bets are off.]<<<<<
—Zeeber (14:27:27/3-31-53)

ALARM MONITORING

As a cost-saving alternative to guard patrols, many home owners choose an option known as alarm monitoring. The house alarm system has a direct line to the security provider's headquarters, the local Lone Star precinct, and often to a security team patrolling the area. As soon as an intruder triggers any one alarm system in the house, the monitor alerts each of those teams. Depending on the company, response time can range from minutes to more than an hour.

>>>>>[Now *this* deserves a closer look, because lots of owners won't spring for alarm monitoring. Usually they've got on-site security to respond to an audible alarm, or they hope that just the sound of an alarm going off will scare the intruders away. In both cases, the alarms are autonomous. (Again, refer to the file on corp security.) In other words, the alarm systems have no connection to the Matrix, so a decker can't do much to suppress them.

Alarm monitoring means the alarm systems connect to the LTG grid or some other kind of communication network, which means at least some kind of hookup to the Matrix—which means a decker can blast down the dataline and turn off the alarms, or at least stop them from sending a call to the monitoring agency.]<<<<<
—Claire (14:15:52/1-31-53)

>>>>>[Claire's right about *most* cases, but it's not too tough to rig up a dial-out-only scheme completely disconnected from the home's phone lines. In this case, the decker could crack into the home phone, but still couldn't touch the alarm-monitoring link. To bypass the alarm monitoring system, the decker has to break into the monitoring system *at the receiving end*—the security corp's headquarters or the Lone Star precinct—and suppress the alert there. A really slick decker could figure out what switching nodes, if any, the monitoring system uses, then ambush the alert signal when it comes through. Not easy, but possible.]<<<<<
—Clever Boy (13:14:19/2-2-53)

ASTRAL SECURITY

Though offered by some top security providers, astral security generally costs more than the average subscriber can pay. A certain number of the guards employed by several companies have magical abilities, but the mere presence of a mage or shaman does not necessarily provide astral security. True astral security consists of some combination of the following: watcher spirits, guardian spirits or elementals, wards, other magical barriers, or mages/ shamans astrally patrolling the vicinity.

>>>>>[No wonder astral security costs. Watchers are easy enough to summon, but they don't stick around that long. Spirits and elementals stay on the job longer, but they're tough, and tiring to summon and bind. Medicine lodges are expensive to set up and limited in size, while hermetic circles only serve as barriers as long as somebody's working inside them.

Wards offer by far the best option. They're fairly easy to bust through, and they have to be reset every few days, but they work.]<<<<<
—Baylis (07:42:17/4-1-53)

>>>>>[Even wards get bloody expensive. In materials alone, any ward worth having costs thousands of nuyen per week. And setting up a *really* strong ward can drain the drek out of a mage, so you can bet he'll ask a hefty price to do the job.]<<<<<
—Pentecost (21:19:51/4-6-53)

>>>>>[I have heard that several corp big-wigs have hired hermetic mages to summon and *permanently* bind elementals to guard their homes. Considering the cost to the mage in terms of karma and energy drain, the fee for such a service must be astronomical. Then again, many upper-echelon corp execs simply cannot find enough ways to spend their money. Poor dears.]<<<<<
—Copperfield (16:51:59/5-13-53)

>>>>>[In his inimitable, pedantic style, Copper's made an important point. The real rich folk, the ones most of us have an interest in, will have paid the piper for some degree of astral security. You probably won't see a fire elemental bound to guard a house in the burbs, but they'll be waiting in the luxury enclaves. Keep that in mind.]<<<<<
—Toshiro (16:29:21/5-26-53)

BIOLOGICALS

"Biologicals" refers to the use of normal or paranormal animals as guards and as deterrents. Security providers must apply for and receive special licenses to use paranormals. Companies currently authorized to use paranormals appear in the company analyses on p. 70. Paranormal animals provide several obvious benefits in addition to their considerable intimidation factor. For example, a dual-natured creature can provide both mundane and significant astral protection and so does not require additional back-up.

>>>>>[Bloch is not authorized for paranormals, but that company's got something I've never seen anywhere else: cyber-enhanced doberman watchdogs. I've seen 'em, and they scare the drek out of me. Cyber eyes, probably with thermo or low light, and they move so fast I think they've got wired reflexes. Scar-y!]<<<<<
—Yuki (16:21:49/2-26-53)

>>>>>[*Bulldrek!* You can't metal up a watchdog.]<<<<<
—Sheaffer (11:20:43/3-10-53)

>>>>>[*Sure* you can, Sheaf. The trick is keeping it under control afterward. But for a free-range watch animal, the kind that just prowls a fenced-in enclosure and chews up anything that crosses its path, that's not a problem.]<<<<<
—Doc (23:25:34/3-14-53)

>>>>>[I've seen some of Bloch's doggies, and I back Doc. Those things are fast, and they're *psycho.*]<<<<<
—Geist (04:47:26/3-15-53)

>>>>>[Where'd you see these things, Geist?]<<<<<
—Arlene (11:45:50/3-19-53)

>>>>>[A shoreline estate out in Madison Park, just off Beach Place. Probably a good place to stay away from.]<<<<<
—Geist (02:14:56/3-24-53)

>>>>>[Maybe…]<<<<<
—Arlene (12:04:44/3-28-53)

EXTENDED PASSIVE DEFENSE

Extended passive defense refers to countermeasures against physical intrusion that function independent of any active decision-making by electronics or (meta)human operatives. The electric fence remains the most common, and is generally a very effective form of passive defense. More expensive, and thus less common, are various laser intrusion-detectors.

>>>>>[I know a couple of places in the Beaux Arts Village enclave that run a two-step laser system: a low-power mode for detection, then a high-power pulse to toast whatever broke the detection beam. (Roger described this technology in the file on corporate security, p. xx.) Some people use lasers to interdict their grounds: lasers on top of the walls, or just inside the fences, but this seems kind of stupid to me. Outside just isn't like a building. Inside a building, you can keep the air clean enough to make the beam invisible. But outside, dust and smog and fog and other crap scatters the light, making the beam easy to spot. This holds just as true for UV and IR lasers as it does for visible light. This system has other problems, too. In order to interdict your back yard you need longer beam paths, and there are fewer available surfaces to bounce the beam back and forth multiple times. So, instead of getting the impenetrable laser "lattice" you might find in a corporate hallway, you get one or two beams you can step over or crawl under.]<<<<<
—Ragnarok (10:37:22/2-20-53)

>>>>>[If you spot the beams.]<<<<<
—Noël (19:38:08/2-23-53)

>>>>>[Let's talk electric fences. In the most common form, the juice is always running. Your average fence carries a punch of about 2,000 volts, the level they once used to kill people using the electric chair. If you touch the fence while grounded, either with flesh or with something conductive, it'll toast you. And face it, most things will conduct 2,000 volts. Even if you live through it, likely your cyberware won't.

On the trid, or in simsense chips, the hero or villain gets away with attaching jumpers to fences to take out a section of the circuit so they can cut through the wire safely. Too bad that doesn't work in real life. Even if you don't cook yourself trying to put the jumpers on, every electric fence ever built sounds an alarm the minute it detects a change in resistance. If anything larger than, say, a cat touches the fence, that sets off alarms too.

Basically, the only way to defeat an electric fence is to go over (or under) it without touching it, or to cut the power. Of course, cutting the power alerts everyone inside that something's going down.]<<<<<
—Sue (10:56:23/3-1-53)

>>>>>[A chummer of mine told me how his team went through an electric fence somewhere in Fort Lewis. His decker killed the power for one minute, they cut the fence, got through, then closed the fence again with metallic twist-ties. Then the decker turned the juice back on.]<<<<<
—Quincy (23:10:57/3-13-53)

>>>>>[Sounds doubtful to me. The cut fence and those twist-tie things would have a slightly different resistance than an uncut fence. The system would have detected it and sounded off.]<<<<<
—Robson (13:41:52/3-14-53)

>>>>>[If the decker can shut down the juice without triggering an alarm, he or she could easily recalibrate the system so the fence read the resistance with cut wires and twist-ties as normal.]<<<<<
—Sue (11:01:29/3-21-53)

>>>>>[That possibility raises an interesting point. An electric fence around a corp facility can be easier to bypass than one around a private home, for the simple reason that the corp fence probably connects to a central computer system, which in turn probably connects to the Matrix. If so, a decker can go in and have his way with the system. Private homes tend to use stand-alone systems that a decker can't get around.]<<<<<
—Claire (01:11:01/3-24-53)

>>>>>[Monowire strung along the top of a wall or fence provides another nasty kind of passive interdiction. Climb the fence or the wall, reach the top safely, step forward to jump down the other side, and lop both legs off on a couple of strands of monowire. Not fun.]<<<<<
—Sue (11:16:41/3-29-53)

>>>>>[Can you run high-voltage electricity through monowire? An electrified monowire fence?]<<<<<
—Lemans (17:28:11/4-3-53)

>>>>>[No.]<<<<<
—Traynor (21:42:52/4-7-53)

LETHAL FORCE

Not all full-service security providers possess licenses to use lethal force. This means that employees of a company without a lethal-force license can shoot to kill, but *only* in personal self-defense. A lethal force license relieves the company's personnel of this constraint.

>>>>>[This bears repetition, boys and girls. Consider a lethal force license legal permission to shoot first and ask questions later.]<<<<<
—Sue (12:18:40/3-21-53)

>>>>>[A lethal force license comes very close to creating a free-fire zone, but stops just short. A sec-guard who geeks an intruder has to prove that the guy he geeked actually *was* an illegal intruder, otherwise the guard gets tried for murder. A guard can't geek you for lurking around outside the fence, because he can't prove your illegal intent. *But*, as soon as you come over the fence, he can blow your brains out with impunity. He doesn't have to yell freeze, he doesn't have to identify himself or otherwise warn you, and he *doesn't* have to shoot for the legs.

In contrast take a guy *without* a lethal force license. You come over the fence. The guard has to identify himself and warn you: "Fargo Security! Freeze! This is a restricted area!", and all that drek. If he sees you go for a gun, he can geek you, but otherwise he lands in big trouble.

If his company has a lethal force license, a sec-guard can lie in wait for you, hidden behind a tree so you can't see him, then pop you the second you step onto guarded property. You'd never know what hit you, or even that anything had. That's kosher. But a guy without an LF license can only pull that kind of sniper trip by using a non-lethal weapon, like a Narcoject rifle or a netgun.]<<<<<
—Lagavulin (11:57:28/4-5-53)

LOCKSMITHING

Locksmithing service allows owners to update the locking mechanisms on all doors and windows in their residence. If appropriate, this service also extends to gates. All full-service providers offer locks of various levels of effectiveness, from the simplest maglocks to sophisticated systems incorporating retina scans.

>>>>>[You're not going to see too many retinal-scan locks in homes, even among the corporate elite. These systems fall to a point of diminishing returns relatively quickly because the aggravation level usually outweighs the increased security. Only the most paranoid corp-types set their security systems to require a retina scan—which takes, what? five seconds or longer?—for their own back door to open for them. On the other hand, Seattle seems to breed paranoids almost as fast as it does devil-rats, so who knows?]<<<<<
—Diamond Jack (11:52:50/2-16-53)

MUNDANE PATROL

At the mention of home security, most people immediately think of armed and armored security guards patrolling the property. Though expensive, physical guard patrols remain popular, particularly within high-class enclaves such as Madison Park. Operatives from licensed and bonded security companies, including all the full-service providers, may carry lethal weapons up to and including submachine guns, though most enclaves do not permit security personnel to carry personal explosives.

>>>>>[Companies like Wolverine and Hard Corps don't give a frag about what's *permitted*. They pack grenades if circumstances warrant.]<<<<<
—Sue (14:20:59/2-16-53)

Quality of personnel training and equipment varies widely.

STRUCTURAL HARDENING

Structural hardening refers to the practice of reinforcing doors, windows, and walls to make them bulletproof and difficult to break down. In the simplest form of structural hardening, the security provider backs all walls and doors with reinforced impact plastic or ballistic composite. Windows present a special difficulty because they must stay transparent, and though some companies continue to use reinforced armor glass to harden windows, new, cutting-edge fiber-plastic weave composites have made significant inroads into the market. These materials offer the hard-cover protection of reinforced impact plastic while providing transparency near that of armor glass.

>>>>>[The only disadvantage to fiber-plastic weave composite is the fact that it costs about 15 times as much as armor glass: 1,500¥ per square meter or thereabouts.]<<<<<
—Sue (11:43:42/3-1-53)

Most companies add bars across windows as part of a residence's structural hardening.

>>>>>[Very few people go for barred windows anymore. Hard-mounted bars stop people getting *out*, particularly in case of a fire, as much as they stop people getting *in*. And if you go for the quick-release style, mechanical or electronic, most likely your friendly neighborhood burglar's got a mage on tap who can remotely release the bars. I think people use bars more for show than anything else nowadays.]<<<<<
—Noël (23:46:45/2-14-53)

COMPANY RATINGS

The Private Security Companies Table provides an overview of the capabilities and services rendered by 13 different companies specializing in security for the private sector.

PRIVATE SECURITY COMPANIES TABLE

	Lethal Force	Alarm Response	Computer Security	Paranormals	Astral Security	Passive Defenses	Active Defenses	Personnel Quality	Mages on Staff	Cost Range
Bloch Security Services	Y	15 min.	B	N	N	Fences	Y	B	Y	B
Desert Storm Security	Y	15 min.	B	N	N	Fences, Lasers	Y	B	N	A
Fargo Security Providers	N	15 min.	C	N	Y	Fences	N	C	Y	C
Hard Corps Security	Y	10 min.	B	Y	Y	Fences, Lasers	Y	A	Y	D
Hartford Security	N	20 min.	B	N	N	N	N	C	Y	B
Jolly Roger Security	Y	20 min.	C	Y	N	Fences	N	D	Y	B
Knight-Errant	Y	10 min.	A+	Y	Y	Fences, Lasers	Y	A	Y	B
Len Grubb and Assoc.	N	25 min.	A	N	N	Fences, Lasers	Y	A	N	A
Nightdancer Home Protection	N	20 min.	B	Y	Y	N	N	B	Y	B
Olympic Home Defense	N	10 min.	B	N	N	Fences	Y	B	N	C
Sydney Services	N	25 min.	C	Y	N	Fences, Lasers	Y	C	Y	C
Wolverine Security	Y	5 min.	A	Y	Y	Fences, Lasers	Y	A	Y	A
Zero-Zone Security	N	25 min.	A	N	N	Lasers	Y	B	N	B

PRIVATE SECURITY COMPANIES TABLE KEY

Alarm Response: The average elapsed time before a team responds to a monitored alarm.

Computer Security: The level of security on the monitoring system at the company's headquarters. Each letter represents how difficult the system makes it for a decker to break in and interfere with normal monitoring functions.

    A—Red-7, Barrier 5, Blaster 5
    B—Orange-6, Barrier 5, Trace and Burn 5
    C—Orange-4, Barrier 4, Trace and Burn 4
    D—Orange-3, Barrier 3, Trace and Dump 3

Personnel Quality: *Consumer Bulletin* uses this subjective grade to rate the training quality and equipment used by the company's on-site security personnel. A denotes the highest level, D represents the lowest.

Many companies also hire combat mages or physical adepts. Company-employed mages generally cast and maintain spells on their comrades as well as themselves.

Cost Range: The cost for security services varies widely, depending on the exact nature of services purchased. As a guideline, *Consumer Bulletin* defines cost range C as "average." Cost range B is twice cost range C, and cost range A equals three times cost range C. Cost range D equals 75 percent of cost range C.

For example, assume that a package of services offered by Fargo Security Providers Inc., a cost range C company, costs 1,000¥ per week. From Desert Storm Security Services, Inc. (cost range A), the same package costs 3,000¥ per week. Bloch Security Services, Inc. (cost range B) charges 2,000¥ per week, and Hard Corps Security, Inc. (cost range D) charges 750¥ per week.

>>>>>[Okay. Here's an example of how all these things come together. I'll describe a place I had cause to, um, visit in Fauntleroy.

First, the perimeter. Its brick-facade walls, 3.5 meters high and 30 centimeters thick, could stop anything short of a t-bird primary gun or a missile. The top of the wall featured inset pressure pads, plus two strands of monowire above. Security guards inside the house controlled the reinforced ballistic composite gate electronically. (And no, the gate circuit didn't connect in any way to the Matrix.)

Inside the wall, a couple of attack-trained rottweilers (no cyber that I could see) and a hell hound patrolled 10 meters of open space. (I guess somebody trained the hound not to eat the rottweilers.) Past that lay a 3.5-meter-high fence charged with 2,000 volts of juice, topped with three strands of monowire. The heavily reinforced fence gate could stand up to any punishment but a heavy vehicle with a running start. But because some bright designer offset the gate in the wall and the gate in the fence by about 20 meters, that running start isn't available. Just as with the main gate, the fence gate tied into a sealed land-line link to the main security booth in the house.

The doors and windows all connected to perimeter alarms. Every door used a thumbprint-keyed maglock, the best money can buy. All the locking systems were autonomous, preventing a decker from trying to crack in through the Matrix. A conductive layer coated the doors and the windows on the inside, juiced with a low-voltage current that was disrupted if anyone cut through that layer. Any disruption sounded an alarm. The doors were constructed of ballistic composite, the windows

of fiber-plastic weave composite. The outside window frames were protected by built-in two-step IR lasers placed to crisscross the window. Laser capacitors discharged when the beam was broken, pumping enough joules into the laser to melt a cyberarm. Two-step IR lasers also ran all around the eaves, so in order to get up onto the roof, an intruder was forced to deal with those lasers.

Personnel-wise, almost a dozen security people guarded the place. I'd categorize them as "class A," using *Consumer Bulletin*'s terminology: armed to the teeth and well-trained. At least two of them were magically active, though I never saw them patrolling astrally. But then, they didn't have to.

A fire elemental and an air elemental prowled around the place, both tough as hell and looking for trouble. A watcher also flitted around, ready to scream for help if something started slotting around with the elementals.

Assuming you survived the trip across the grounds, the inside of the the house held its own bag of tricks. Low-power, alarm-type lasers and pressure pads crisscrossed key hallways.

The place belongs to a *real* corp highlight, a prime target for a lift-out attempt. Needless to say, his security company provided terrific defenses against air assaults, beginning with a small phased-array system on top of the house that constantly swept the airspace above it with radar. (The array ran off its own electrical circuit, and the whole house could run on emergency generators.) If the radar picked up something unauthorized it triggered an air-defense emplacement up top: a Vindicator minigun on a servo mount, slaved to a command system in the guts of the house. (I don't think the Vindicator had line-of-fire to the grounds, but I wouldn't swear to it.) Presumably, if the guns missed, the elementals got the chance to mess up any unauthorized aircraft making final approach. (I would *not* like to try landing a light craft while dodging minigun fire and tangling with a fire and air elemental in the same five minutes.)

I made it in and out again, but I won't tell you how I did it. Let the reader figure it out.]<<<<<
    —Victoria (15:38:09/5-11-53)

>>>>>[Pedantic scag.]<<<<<
    —Rox (11:03:39/5-23-53)

>>>>>[What about metal detectors and chem-sniffers? Nobody's mentioned them.]<<<<<
    —Manitou (13:04:12/12-11-53)

>>>>>[Sometimes you find them in the entry halls of mansions. A chummer told me about one place that built detectors into two old suits of armor that flanked the hallway.]<<<<<
    —Quincy (01:15:41/12-25-53)

>>>>>[This whole discussion of security companies misses the point. The rich corporators usually have corp security looking after their personal places. Anyone else needing serious security is just as likely to hire private operators—ex-shadowrunners, or runners down on their luck at the moment. You just can't predict with any degree of accuracy what kind of security you'll run into if you decide to break into some guy's place.]<<<<<
    —Debbie (05:32:14/12-30-53)

NELSON

SHARPER IMAGE

Reprinted from Razor's Edge Catalog, *Spring 2052*

The *Razor's Edge Catalog* brings you what's new to sharpen your image and keep you on the cutting edge of fashion and tech. Spring 2052 is a great time to update your look and your life—time to impress everyone from your boss to your corp sec-guard to the women you meet and the bully boys who look at you as a target. Take charge of your appearance with our nuyen-back guarantee, and take control of your life!

>>>>>[I left a whole drekload of this stuff in the last *Real Life*. This time I've edited out the soap and depilatory and fruit baskets and sludge like that, and tried to cover the products street ops like yourselves might conceivably take an interest in.]<<<<<
—Captain Chaos (01:44:20/1-8-53)

WHITELAW ELECTRIC SUNGLASSES

Resin-composite lenses change their polarization depending on the current flowing through them in the newest line of sunglasses from trend-setting Whitelaw. Their innovative filtering system guarantees that an even level of brightness reaches the wearer's eyes regardless of the incidental light. In bright sunlight, the lenses darken to exclude 99.9 percent of damaging ultraviolet rays, also eliminating glare and dazzle. Under night-like conditions, the lenses still eliminate dazzle—for instance, from oncoming car lights—as they enhance contrast and depth perception. Optically perfect, the Whitelaw line comes in any diopter strength for required vision correction. (Starting at 250 ¥.)

>>>>>[Can these things provide cheap flare compensation?]<<<<<
—Stacey (17:34:15/2-23-53)

>>>>>[No. They don't respond fast enough. By the time the lenses change polarization, you've already been flash-dazzled.]<<<<<
—Orson (09:11:35/2-27-53)

CORONA "PRIVATE EYE" COMPUTER DISPLAY GLASSES

Corona Data Corporation announces the first major break-through in computer data-display technology in two decades. The "Private Eye" system resembles a pair of partially mirrored eye-glasses, with a hairline optical fiber running from the earpiece to the thumbnail-size interface unit which connects to the "data out" jack of a telecom or pocket computer. Connected, the "Private Eye" blanks out the computer's data display and projects the image on the inside of the "Private Eye" glasses. As with vehicle head-up displays, the image fills the wearer's visual field. Though clearly visible even in bright sunlight, the transparent display does not interfere with the user's normal vision. The "Private Eye" offers the perfect solution for the problems of "commute-computing," as well as the ultimate privacy.

Compatible with all telecoms and pocket computers. (Save 150¥. Now only 1,150¥!)

>>>>>[This is a pretty good product. If you worry about people looking over your shoulder while you work, or if you want to work in the car on the way to your office, this toy fits the bill.]<<<<<
—Lee (14:17:44/3-24-53)

>>>>>[Just jack in!]<<<<<
—Neon Cowboy (10:30:11/3-27-53)

>>>>>[Not everybody's got a datajack. And sometimes you need to see what's on the screen and what's going on around you at the same time.]<<<<<
—Lee (16:09:42/3-28-53)

>>>>>[It took me a while to get used to this thing's beta release. At first it gave me crippling headaches. Then I learned to mentally "fade to black" either the computer image or the real world, whichever I didn't want to pay attention to at the moment. No matter what the adverts say, driving a car wearing this thing doesn't show too many smarts. But this gadget has lots of other applications.]<<<<<
—Harry J (23:05:48/3-28-53)

FELLINI-MED BREATHER

This new particulate matter filter cleans the air you breathe using electronic precipitation, and the new-for-'52 Fellini-Med Breather improves on the winning design of earlier Fellini-Med products. The new model has a lower profile, and its more flexible material softly cups the mouth. A gentle clip of patented SoftTouch™ holds the nose closed. Completely self-contained, the Fellini-Med Breather dispenses with intrusive, ugly battery packs. A single 4mm Geltech™ energy cell powers the Breather for up to 60 days of continuous use.

The Fellini-Med Breather clips neatly onto the lapels of today's high-collar jackets, and comes in a wide range of designer colors and textures.

(Fellini-Med Breathers start at just 350¥, including one Geltech energy cell and two replacement filters. Additional filters cost 45¥ each.)

>>>>>[Beware. These breathers filter out particulates like smog, but they do squat about gases like carbon monoxide or Neuro-stun VIII.]<<<<<
—Nova (16:11:49/2-23-53)

>>>>>[I got a chummer with the disturbing habit of coughing his fragging guts out when he breathes cordite smoke. Usually at the worst possible times, like in the middle of a firefight. We set him up with a Fellini-Med Breather, and it shut him right up.]<<<<<
—Zonk (06:14:31/3-6-53)

STANLEY "SCREAMER" PORTABLE DOOR ALARM

The perfect security solution for business travelers! This 4 x 4 x 1 centimeter unit attaches to the inside of your hotel-room door and detects the characteristic electronic impulses created by any attempt to defeat the door's maglock. A built-in vibration sensor also detects any attempt to physically jimmy the door open. It also reacts if someone opens the door, from the outside or the inside, without first disarming the unit. The Screamer emits a piercing electronic squeal guaranteed to wake and alert the deepest sleeper. From Stanley Security Technologies. (Save 45¥. Now only 450¥.)

>>>>>[This thing detects someone slotting with the maglock only if the maglock keypad or keyslot is built right into the door. How often do you see that?]<<<<<
—Marjorie (18:24:00/3-13-53)

>>>>>[You can adjust the sensitivity of the vibration sensor. If you're real paranoid, it can go so high that it goes off if anyone walks near your door.]<<<<<
—Hersh (22:06:54/3-16-53)

>>>>>[Drek, I like these things 'cause they ring when the door opens, and it'll happen eventually, right? Hang 'em inside the door where the joker trying to get in can't get at it. You may just give yourself the few extra seconds you need to make it out alive.]<<<<<
—Lovable Lou (12:51:43/3-21-53)

FUJICORP REMOTE IGNITION

A great gift for the commuter from Fujicorp of Kyoto! Install the receiver circuitry into your car's ignition, then start the engine from up to 30 meters away simply by pressing a button on a small (3 x 2 x 2 centimeters) transmitter. On cold mornings, you can warm up the engine and heater before you step into the car. More than 4 billion available codes guarantee security. (Save 50¥. Now only 550¥!)

>>>>>[The major corps install these in limos belonging to their execs so a chauffeur can start the car from a safe distance, out of blast range of any car bombs wired into the ignition.]<<<<<
—Hatchetman (18:34:16/2-24-53)

>>>>>[Start your car from 30 meters away. A sneak thief 20 meters away beats you to it, jumps in and drives away. Convenient.]<<<<<
—Post (22:16:33/3-19-53)

>>>>>[It starts the engine. It doesn't unlock the doors, you slot.]<<<<<
—Webster (04:19:21/4-2-53)

>>>>>["More than 4 billion available codes" implies a 32-bit code. That doesn't sound secure enough to me. Maybe I'd consider buying one of these if they implemented a 64-bit code. More than 1.8E19 codes—1.8 x 10^{19} codes—would make me feel a little more secure.]<<<<<
—Shrimp (00:39:34/4-15-53)

DES SYSTEMS PHONESECURE SCANNER

A low-cost alternative to pricey dataline scanners, the PhoneSecure™ from pace-setting DES Systems checks hardwired phone lines for taps and bugs. Jack it into the dataline of the phone to be checked and press the TEST key.* In less than a second you receive the verdict: a green light means the line is clear, a red light signals a tap or bug.

No security-conscious person should be without the PhoneSecure. (Save 15¥. Now only 150¥.)

*The PhoneSecure dataline scanner carries a Rating 2. To determine if it detects a bug, roll 2 dice against a target number equal to the bug's rating. On a single success, the PhoneSecure detects the bug.

If a character uses the PhoneSecure on a cellular phone, roll 1 die against a target number equal to the bug's rating.

>>>>>[Unlike your standard dataline scanner, the PhoneSecure only picks up active bugs. It reads any line with bugs on standby as clean.
On the plus side, it costs less than the standard dataline scanner. And you can pick it up through the *Razor's Edge Catalog* and avoid the hassles of a security equipment provider. Not a bad idea, considering the number of equipment dealers that Lone Star monitors.]<<<<<
—Mercedes (12:09:21/2-13-53)

>>>>>[This thing won't work on cellulars.]<<<<<
—Portia (01:12:09/2-17-53)

>>>>>[It works on cellulars: just not reliably. Oddly enough, it never gives false positives. If the Phone Secure flashes red, you know there's a tap in place. It *can* give you false negatives, though; just because it flashes green doesn't mean you have a clear line.]<<<<<
—Sal (11:45:50/3-2-53)

TOSHIBA WHITE-NOISE GENERATOR

Through the wonders of ultra-microminiaturization, Toshiba introduces the world's smallest white-noise generator. This tiny unit incorporates easily into a ring, belt buckle, pendant, even an overcoat button. Despite its small size, it produces enough amplitude to defeat eavesdropping devices within a one-meter* radius. Only Toshiba offers such unobtrusive, affordable personal security. (Save 100¥. Now only 1,000¥.)

*In the lab on a standard acoustic test-bed, the Toshiba White-Noise Generator tests out at a Rating of 2.

Street users report different results. When incorporated into a piece of jewelry or other accessory and used in standard circumstances, the Toshiba actually performs with a Rating of 1. (Sorry, chummers.)

>>>>>[I've checked this thing out. It actually works. Not well, but it does work.]<<<<<
—Charles (18:11:56/3-1-53)

>>>>>[Yes, but for how long? I hear rumors that the microcell powering it carries only enough juice for 15 minutes of continuous operation.]<<<<<
—Gutter Lark (23:18:10/3-5-53)

DOAFONE LOCK-OUT

Bothered by crank calls and salesmen on your cellular at the worst possible moments? Protect yourself from time-wasters with the Doafone Lock-Out. The tiny Lock-Out module, 1.5 x 1 x 1 centimeters, connects to your cellular's circuitry and monitors incoming calls by comparing the originating number with a list of up to 256 numbers stored in its optical chips. The Lock-Out responds to the call based on how the cellular owner configured the unit.

To use the Lock-Out's "exclusion" mode, enter the originating numbers from which you will not accept calls. If a call comes in from any of these numbers, the Lock-Out overrides your cellular's bell circuit, issues a 10-second outgoing message, and disconnects the call. Your cellular receives all calls from numbers not on the exclusion list.

>>>>>[Also filters calls from your spouse, fixer, or creditors.]<<<<<
—Slag (13:26:29/2-22-53)

Lock-Out's "inclusion" mode accepts calls only from those numbers entered into the unit's number list. The Lock-Out disconnects all other calls after transmitting the 10-second outgoing message.

>>>>>[Note that these two modes are mutually exclusive.]<<<<<
—Burroughs (12:01:42/3-5-53)

The Doafone Lock-Out is compatible with all major cellular designs, and functions dependably with all CCITT Group VI V9.2bis-compliant cellular faxes and 38,400 bps cellular modems. (Save 45¥. Now only 595¥ (installation extra).)

>>>>>[Hardwired phones have offered this function for some time now, and so has the actual cellular network. Of course, to use it you'd have to give the phone company a list of the numbers you wanted to include or exclude, and lots of people feel (rightly, I believe) too paranoid to do that.]<<<<<
—Jeff (13:36:34/3-12-53)

>>>>>[Save some nuyen. I've reverse-engineered this puppy, and can give you the same functionality for 550¥ installed. Call LTG# 16206 (35-1650) and leave a message.]<<<<<
—Bit Basher (23:54:32/3-17-53)

MIKEN 92'

ONE-WAY COMMUNICATION

Reprinted from a public-access paper presented by Anthony Colucci, Dr. Eng., at the International Microtronics Symposium

CONCEPTUAL OVERVIEW

The extreme societal permeation of standard omnidirectional dataline usage nearly warrants active disregard of its parameters in favor of immediate immersion in the subject at hand. However, in deference to neophytes to the subject, a brief overview of said systems follows. Those readers already intimate with the conceptual theory of the omnidirectional dataline can proceed to the contiguous section.

>>>>>[Every city is proud of its intellectual elite. Some might guess that Seattle has nothing to brag about on this score, so I've included this reprint of a paper presented at a recent convention by one of Seattle's very own. This guy seemed a little unclear on the concept, though—this was supposed to make the relatively obscure topic of one-way datalines accessible to the regular Joes and Jills out there. So I edited the drek out of this, and you'll figure out why pretty fraggin' fast. Sure, this kind of techno-geek-speak interests some people (don't avert your eyes; we know who you are), but most of the reading public doesn't give a frag about "sequence dependent transposition"—they'd prefer general information in general terms. If you're into it, hunt down the original article. If you're not, thank me later.

Blake must have included this piece in his version of *Real Life* as an appeal to the other special-interest conventioneers—seems like there's herds of geeks cluttering up the sidewalks and restaurants on a regular basis lately.]<<<<<
—Captain Chaos (01:58:31/01-8-53)

The omnidirectional dataline, as the default dataline format, has warranted little analysis in terms of its capabilities and restrictions. Its operational parameters allow unrestricted, non-interfering, multi-signal data transmission along its length, regardless

of the direction of the transmission. Common connection components all possess multiphasic transfer capability, permitting creation of the non-interfering structure of the dataline. Following the international signal format agreements of 2014 (see the IAMET bulletin MSI1075-A14 *Multiphasic Signal Standards*), the convergence factors applied to the <<**block delete: 7.5Kp**>>

>>>>>[Aw, just when it was starting to get interesting....]<<<<<
     —Shrimp (17:51:46/2-12-53)

>>>>>[I have the original article text. If desired, I can upload it and append it into the existing text sections.]<<<<<
     —Preemptive Pete (09:12:45/2-26-53)

>>>>>[You do that and I will hunt you down and remove your ankles through your ears. Are we on the same wavelength here?]<<<<<
     —Hatchetman (12:56:12/3-3-53)

>>>>>[Affirmative.]<<<<<
     —Preemptive Pete (08:53:12/3-5-53)

In summation, the omnidirectional dataline permits usage and signal transmission from either end, moving in either direction. Such a dataline provides optimal functionality for designs where two-way communication is required between nodes.

UNIDIRECTIONAL DATALINES

The unidirectional dataline, on the other hand, allows data transmission in a single direction complementary to its polarized design. Signals can pass only in the direction of the quantum polarization, transveyance is effectively prohibited against dissonant propagation <<**block delete: 24.8Kp**>>

>>>>>[Okay, in plain English, a unidirectional dataline only lets data flow one way. From the wrong end, you can't use it; you can't get down the line. Brick-wall time. On the right end, no problem: it works like a standard dataline. Simple, really. A lot simpler than they make it sound here.]<<<<<
     —Teach (13:54:15/3-3-53)

>>>>>[Simple in a general sense, yes, but complex in execution. Regular datalines (omnidirectional for the purists) are simple, polymer, fiber-optic lines. Unidirectional lines require customized extrusions. Customizing them makes them much more expensive, and therefore less common.]<<<<<
     —Sinclair (09:43:34/3-6-53)

ICONOGRAPHIC EXECUTION
The existence of a unidirectional dataline can be simply conveyed within the standard iconographic symbol set in the following manner:

Unidirectional Dataline

Standard (omnidirectional) Dataline
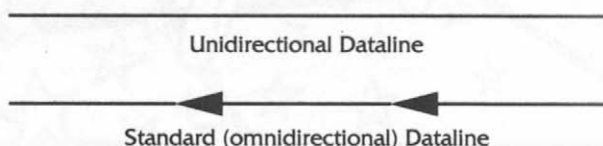
The orientation of the arrow significator indicates the restricted direction of data flow. Data attempting to enter the unidirectional dataline against the quantum polarization will suffer EDR fragmentation <<**block delete: 2.1Kp**>>

>>>>>[BLEARGH!]<<<<<
     —Hatchetman (13:08:01/3-3-53)

>>>>>[Okay, Flat-Symbol Matrix Iconography 101 revisited. If you're looking at a two-dimensional representation of a computer system and a dataline symbol (a straight line connecting two nodes) appears with an arrow in it, data (that's you, decker!) can only move in the direction of the arrow. You can't move against the arrow from the node at the other end. That's it.]<<<<<
     —Teach (14:00:22/3-3-53)

Using a three-dimensional symbol-set, specifically the Universal Matrix Specifications (see *Tokyo '39: The Universal Matrix Specifications Conference Collected Notes*, Fuchi Press Publications, 2039), it is impossible to differentiate between an omnidirectional dataline and a unidirectional line from a representative distance without assignment of a different identifier code series <<**block delete: 1.5Kp**>>

>>>>>[No fraggin' kidding, Columbo. Sometimes, these guys amaze me. See, your cyberdeck can recognize something because each object in the Matrix has a separate identifier code series (ICS) that tells the deck what it is under the UMS guidelines. Obviously, a unidirectional dataline has a different ICS than an omnidirectional one. Drek-headed deckheads.]<<<<<
     —Vince Valiant (09:23:52/3-12-53)

>>>>>[Bad news, Vinny, you're wrong. Datalines don't have UMS ICS codes. When a decker looks at a UMS system, he can't see the datalines. Otherwise, the datalines would obscure just about everything in view in large systems. The data shows up as ghostly trace a decker can spot, and your cyberdeck easily tracks the data's path and gives you a rough dataline echo-image if you ask nice. But no decker can use the UMS system to tell one kind of dataline from the other.
     Can anybody guess how you tell them apart?]<<<<<
     —Teach (22:54:03/3-17-53)

>>>>>[Livin' up to yer name, eh Teach? Okay, enlighten us.]<<<<<
     —Mr. Miracle (03:52:52/3-19-53)

>>>>>[Aw, this is too easy. Answer: YOU LOOK AT IT!]<<<<<
     —Shrimp (08:52:43/3-20-53)

>>>>>[A gold star for you, Mr. Shrimp. You look at it. In a unidirectional dataline, data only flows in one direction. It looks like city traffic from on high, only you won't see any drekhead drivers who can't read ONE WAY signs in the Matrix.
     Of course, depending on the time, you might be watching data flowing in one direction through an omnidirectional dataline by coincidence; say, during a shift-end back-up or something. But you guys get the big bucks to figure that stuff out. Right?]<<<<<
     —Teach (21:55:32/3-21-53)

>>>>>[Editorial Note—I pulled the rest of the actual text when it became apparent that the shadowtalk gave far more useful information than the actual article. Again, if you have any questions, check out the original or post here.]<<<<<
—Captain Chaos (07:56:51/9-14-53)

CUSTOM MULTISYMBOL ICONOGRAPHY

<<block delete: 13.5Mp>>

>>>>>[Wow. Okay, I think I followed that. Check me: In a sculpted system the one-way dataline looks like something that takes you in only one direction. For example, a slide, a chute, a turnstyle, or something similar. That right?]<<<<<
—Shrimp (18:09:36/2-12-53)

>>>>>[Exactly.]<<<<<
—Teach (21:51:24/2-18-53)

>>>>>[If it's that simple, HOW COME HE TOOK THIRTEEN AND A HALF FRAGGIN' MEGAPULSES TO SAY IT?]<<<<<
—Shrimp (07:42:31/2-20-53)

>>>>>[Don't blame the author, he was bred that way.]<<<<<
—Shane (23:53:41/3-1-53)

>>>>>[Saw a kinda neat example of a unidirectional dataline "out" point recently. I'm in somewhere, no names please, strolling down a long marble-and-chrome hallway. Really hi-rez, by the way. As I'm ambling, I pass a door labeled "Exit Only." Kinda wiz, eh?]<<<<<
—Tokyo Tom (01:32:34/3-10-53)

>>>>>[Hey, were you the black and green cyberturtle with a funky ray-gun turret on its back, standing there gawking when I came barreling out? If so, my apologies, chummer. Thanks for distracting one of the Saeder-Ks. I owe you a brew.]<<<<<
—Adder (10:15:53/3-11-53)

>>>>>[No problemo. You can pretty much always find me in Elysium when I'm not on a run (or re-cooking melted chips).]<<<<<
—Tokyo Tom (03:12:32/3-13-53)

APPLICATION

<<block delete: 2.2Mp>>

>>>>>[I've uploaded a few examples of interesting uses for unidirectional datalines within a system. Most people probably already thought of this first one: an output-only I/O port. The signal only travels one way down the dataline, which stops anyone from jacking into the system through the printer (or whatever) port.

SYSTEM EXAMPLE A:

Here's a similar concept: a write-only datastore. The system can dump data to this node, but can't retrieve from it. Particularly useful for back-ups and such. Note that anyone traveling down a one-way dataline into one of these puppies can return to the previous node, but can't download any data (no retrieval). Lotsa fun, eh?

SYSTEM EXAMPLE B:
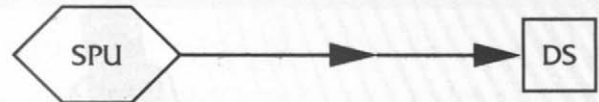
I stole this complex little execution from a Seattle system, namely the security cluster of a mid-sized local corp. This example represents the decentralized paradigm recently being applied to security systems as discussed earlier in this file series. Get used to it. I expect it to become more popular.

SYSTEM EXAMPLE C:
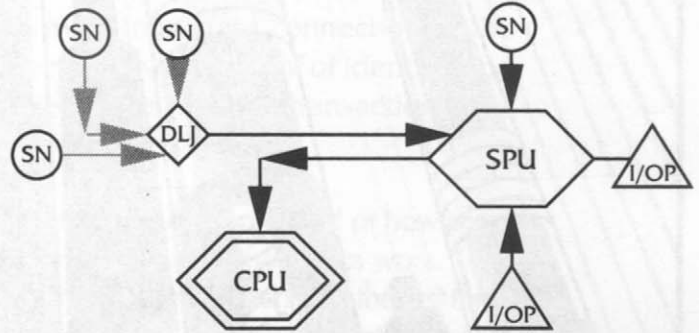
Pay attention. You will be tested on this material later (especially if you're a decker!).]<<<<<
—Teach (20:53:48/3-27-53)

>>>>>[I recently saw a set-up that is, so far, unique to the Fuchi mainframe in Japan. A variable polarization dataline, it takes commands from an SPU at one end to flip-flop between directions so that sometimes data can only come in, and sometimes only go out. An interesting set-up with interesting ramifications.]<<<<<
—FastJack (04:12:59/4-2-53)

>>>>>[Isn't that basically how access IC works? Or barrier IC?]<<<<<
—Shrimp (14:39:56/4-3-53)

>>>>>[Yes, but access or barrier IC carries accessible control inputs. A good decker can sleaze, deceive, or fight access or barrier IC. On the other hand, a variable dataline isn't flowing your way and the SPU lies on the other end, you're stuck.]<<<<<
—FastJack (14:29:55/4-6-53)

>>>>>[Oh joy joy.
By the way, you chummers notice how casually he tossed off "saw in the Fuchi mainframe in Japan?" Gawd.]<<<<<
—Shrimp (23:29:16/4-7-53)

YOU ARE YOUR CREDSTICK

Reprinted from New School Review, *September 2052*

I n many ways, a credstick is a person's single most important connection to the world. It controls access to his or her bank account, serves as proof of identity, and provides emergency medical information. A credstick's financial transaction function, however, sees the most use.

>>>>>[Inasmuch as we all exist in this modern world, I am often amazed at how some people seem to drift through life with little understanding of how the basics work. Take credsticks. We all (well, most of us) use them every day, but don't understand the first thing about how they work. This article appeared originally in a datamag targeted at new freshmen in the high schools connected to the DataNet education system.]<<<<<
—Captain Chaos (02:12:48/1-8-53)

ACCESSING MONEY

The optical chip integral to credsticks contains coded information allowing any reader initial access to the financial records attached to that credstick. Beyond the most recent balance information, the stick itself stores no actual financial data, only the access codes.

>>>>>[Right. The money stays on file somewhere, nice and safe. So if you lose your stick, or heaven forbid, it gets stolen, CHANGE YOUR PASSCODE right away.]<<<<<
—Amin (21:18:52/3-8-53)

Upon scanning an inserted credstick, the credstick reader connects to the appropriate financial institution and allows the holder to manipulate his or her

account(s) by depositing, withdrawing, or transferring funds. Access to account information is not automatic. Depending on the type of credstick being used, some level of identification may be required to open financial records.

>>>>>[Something I learned from dissecting a credstick: the stick itself doesn't carry all the passcode data on file. Most of the code is stored with your financial records, so if you "find" a platinum credstick just lying around, you'd be better off trying for a reward than trying to use it.]<<<<<
　　—HepCat (09:16:48/3-9-53)

TYPES OF CREDSTICKS

Credsticks come in five types distinguished by the amount of funds each can access and the amount of identification cross-referencing information each requires for use:

Standard Credstick	1–5,000¥
Silver Credstick	1–20,000¥
Gold Credstick	1–200,000¥
Platinum Credstick	1–1,000,000¥
Ebony Credstick	Unlimited

Banks issue credsticks based on complex calculations involving the account owner's credit history and projected average daily balance.

>>>>>[Yeah, it's worth the price of admission to see a corp's face when the bank calls him asking for their ebony credstick back 'cause his account suddenly has a zero balance. "You did authorize the transfer of those funds to the Caribbean League, didn't you, Mr. Corp?"]<<<<<
　　—Hatchetman (09:27:34/2-27-53)

IDENTIFICATION LEVELS

Credsticks also serve as identification. Most major local, state, federal, and corporate agencies recognize credsticks as proof of identity. Furthermore, the more money the credstick can access, the more extensive the type of ID attached to it, and the more complex the verification process required to use it. Each of the five levels of credstick requires an additional level of ID verification, but these ID levels are not necessarily cumulative. In other words, an ebony credstick does not require all five ID checks, but does require those most difficult to fake or break.

Passcode

A passcode is a simple, alphanumeric code consisting of up to 30 characters required for all standard transactions. Standard credstick reader designs all offer small keypads for passcode input. Some credsticks come with integral pressure-sensitive pads to allow passcode input.

Fingerprint

For ID confirmation requiring a thumbprint, the credstick holds a copy of the print and compares it with the print on file at the financial institution.

Voiceprint

Often taken passively through a pickup microphone in the credstick checker's area, a voiceprint ID does not require a specific "voiceprint statement," but usually requires the holder to speak at least ten words in addition to prepositions and place holders. Most institutions require a passcode in addition to the voiceprint.

Retinal Scan

When taking a retinal ID scan, the reader compares a detailed scan of the bearer's retinal pattern with the master on file at the financial institution. This verification also requires a passcode.

Cellular Scan

A user conducting a large transaction may have to undergo a cellular scan in addition to a retinal scan and passcode check. The scanning process requires only a small cellular sample, such as a bit of skin.

>>>>>[Hey, wait a minute...]<<<<<
　　—Shrimp (13:52:51/3-2-53)

>>>>>[I think I can read your mind, little shrimper, but have no fear. Analysis destroys the cell sample; only the data profile stays on file. Cell samples don't get stored anywhere, so mages have nothing to worry about.]<<<<<
　　—Keefe (9:12:34/3-4-53)

>>>>>[Yes, but in order to use a forged credstick with a bogus background attached to it, I have to provide something legit: a fingerprint, voiceprint, retinal print, or cell structure file. For all you paranoid folk out there, that means a trail of sorts points back to you. For instance, if somebody ran the prints taken from your sloppy last run against prints from all the active credstick accounts in the Seattle area, they could find a match...]<<<<<
　　—Hatchetman (21:49:40/3-9-53)

>>>>>[Yeah, and they'd have to borrow the processor time of every computer in Seattle to do it.]<<<<<
　　—Snowman (06:56:54/3-17-53)

>>>>>[Not at all. Data storage algorithms are pretty sophisticated. You really only need to store the deviation information and compare that with the sample. The real problem in conducting this type of search is that corporations control all the fiscal-related ID information, and (fortunately) they won't agree to using their files to hunt down their own customers.]<<<<<
　　— Teach (14:42:19/3-21-53)

USING A CREDSTICK

If a person wished to use his or her credstick to purchase a new simsense deck from the local microtronics store, he or she would authorize payment by inserting his or her credstick into the store's credstick reader/transfer system. The system connects with the holder's financial institution, then prompts the user to provide identification based on the level of the transaction in progress.

The Credstick Transaction ID Table shows the identification required to process a transaction at a specific level of nuyen. It also shows the minimum credstick type carrying that level of identification information.

CREDSTICK TRANSACTION ID TABLE		
Transaction Amount	**ID Required**	**Credstick Type**
Up to 5,000¥	Passcode	Standard
Up to 20,000¥	Fingerprint	Silver
Up to 200,000¥	Voiceprint	Gold
Up to 1,000,000¥	Retinal Scan	Platinum
1,000,000¥+	Cellular Scan	Ebony

After verifying identification, the store's transaction system institutes a transfer of the appropriate funds from the credstick to the store's account. It then downloads an electronic receipt to the credstick, and the customer heads home with the simdeck.

OPENING AN ACCOUNT

To open a credstick account, the financial institution requires a customer to provide his or her System Identification Number and to supply identification information appropriate to the level of credstick issued.

Many people carry multiple credsticks representing accounts at different financial institutions. Others prefer to consolidate all their account records on one credstick for convenience.

Most financial institutions also provide certified credsticks. Like cash or a bearer bond, the certified credstick is worth the amount encoded and requires no identity verification to use. The issuing financial institution encodes the stick with raw funds, money that exists only on that credstick. A certified credstick can be used by persons other than the individual for whom it was originally issued. Most financial institutions charge a small fee to create a certified stick, usually 2 to 5 percent of the credstick amount. Certified credsticks cannot be used to establish or verify an ID. Some or all of the funds on the certified credstick can be transferred to another account, and new funds can be transferred onto the same stick, up to the fiscal limit imposed by the type of credstick.

All institutions accepting credsticks use credstick checkers to verify the existence of the claimed account and the owner's identity. Transaction and verification systems use elaborate evaluation and cross-referencing software to confirm the identity of the owner. Though inconvenient, these measures exist for the consumer's protection.

>>>>>[These days, the standard credstick actually functions as two sticks in one. Part of it contains the standard credstick coding, and the other part can be used for storing certified funds. Convenient, really.]<<<<<
—Gizmo (12:56:13/3-12-53)

>>>>>[Stick-to-stick transfers, though possible, can only be made between certified funds. Transfers from a regular account to a certified portion of a credstick can take place at any automatic transfer machine (ATM). Stick-to-stick transfers of non-certified funds cannot be confirmed (or considered to have taken effect) until both sticks have next connected with their respective financial institutions, which can get risky.]<<<<<
—O'Bert (18:58:17/3-19-53)

RULES

Not in my game you won't!
—*archetypal* Shadowrun *gamemaster*

T his section provides game rules and stats for the products and systems discussed in the articles that make up **Real Life**, including new vehicles and NPC Archetype stats. These rules are for use with both the original **Shadowrun** system and the **Shadowrun, Second Edition**, rules. SRII stats appear in {**boldface brackets**}.

SECURITY SYSTEMS

Every homeowner, small businessperson, and corp head of security uses different security precautions to protect their area of authority; corporations, offices, research facilities, homes, and personal territory. The following information on various forms of security is provided for those gamemasters who want to make penetrating a security system more realistic. Players may even want something more challenging than, "Roll your Electronics skill against the security system's rating of 4." Gamemasters can use this information to decide exactly how the security system works, and require the players to explain, step by step, how their characters will attempt to defeat it.

Gamemasters and players alike will quickly realize that some security subsystems, and combinations of subsystems, are quite literally impossible to defeat without the use of magic—or even *with* magic. And that's okay. Some things shadowrunners just shouldn't be able to get at easily. Just remember that there are more ways to circumvent a security system than simply crashing it. Characters may be able to use a few less physical skills to penetrate a system: *somebody* has to go into the secured area at some time. It may just be a matter of snatching that person, having a chat with them using blunt objects, and finally obtaining the necessary passcodes, cards, or whatever.

Actually running a security system can add a lot more interest, intrigue, and complexity to an adventure. Of course, gamemasters who prefer a less complicated run can still handle the whole thing by rolling the dice.

KEYPADS

Keypad systems carry standard Ratings from 0 (available at local electronics stores) to 6 (custom-designed systems). Unless the character knows the access code, he or she can only defeat a keypad by rewiring the internal electronics. This requires two steps, removing the casing and tampering with the circuits.

Breaking A Keypad

First, the runner must remove the keypad casing. This requires a successful Electronics (B/R) Test against a target number equal to the Barrier Rating of the casing. Usually, the Barrier Rating of the casing is equal to the rating of the actual keypad system. It is possible to install a keypad system of one rating in a casing of a different rating, but the cost of the procedure is too prohibitive to make this a standard practice. All but the very high-end security systems will have a keypad and casing of equal rating.

The character must generate at least 1 success to remove the casing. Failure to generate any successes simply means that the character could not remove the casing. This task requires a base time of 60 seconds, and extra successes may be used to reduce the base time per the standard rules (see page 56 of **Shadowrun**, or page 68 of **Shadowrun, Second Edition**).

The character adds the rating of any anti-tamper alarm system attached to the casing to his or her Electronics (B/R) Test target number. Anti-tamper systems are usually rated from 1 to 4. The character must generate at least 1 success to defeat the anti-tamper system and remove the casing. Failure to generate any successes in this case sets off the alarm.

In order to avoid revealing too much information to the players, the gamemaster should keep the target number for this test a secret, and simply indicate success or failure as appropriate.

Once the character breaches the keypad case, he must now tamper directly with the keypad circuits. Resolve the success or failure of this effort using a standard Electronics Test against a target number equal to the rating of the keypad system, plus 2. The character has a base time of 60 seconds, must achieve 1 success to override the alarm, and may use any additional successes to reduce the base time required for the task. Failure to achieve any successes means that the computer system controlling the keypad noticed the penetration attempt and triggered a passive alert.

For both the above tests, apply the appropriate modifiers from the Build/Repair Skill Situational Modifiers Table found on page 154 of **Shadowrun**, or the Build/Repair Table on page 183 of **Shadowrun, Second Edition**.

Of course, modern technology provides a device to assist in this task, called a sequencer. It is specially designed to feed the security system a series of passcode sequences based on very advanced mathematical algorithms. The device must be attached to the keypad's circuits, however, and so a character using a sequencer must still remove the keypad case. Sequencers are available in Ratings 1 through 6, and cost 500¥ multiplied by the square of the device's

rating (500¥ x Rating x Rating). To defeat the keypad system using a sequencer, roll a number of dice equal to the rating of the device against a target number equal to the rating of the keypad. At the same time, roll a number of dice equal to the keypad's rating against a target number equal to the rating of the sequencer. The sequencer must achieve 1 success to penetrate the system. The base time for this test is 10 seconds, and additional successes can be used to reduce the base time. Ties have no result. If the keypad generates more successes than the sequencer, the monitoring system triggers a passive alert.

CARDREADERS

Cardreaders are normally rated from 1 to 6 and can be defeated using the same method as for keypads, by tampering with the works or applying a special device. See **Breaking A Keypad**, above, for more information. As with keypads, the "guts" of cardreaders are protected by cases that must be removed before the circuits can be tampered with. The target number for the Electronics Test used to remove the casing is equal to twice the rating of the cardreader. The base time for the task is 60 seconds.

A device designed to defeat a cardreader is variously known as a passcard, passkey, or skeleton card. It functions in the same way as the sequencer described under keypads, except that the passcard can be inserted into the same slot used for the legitimate passcard, leaving the case in place. To determine whether or not the passcard deceives the cardreader, roll a number of dice equal to the passcard's rating against a target number equal to the cardreader's rating. The base time for this task is 10 seconds. Failure to generate any successes triggers an alarm.

A maglock passcard costs 10,000¥ times the square of the device's rating (10,000¥ x Rating x Rating).

PRINT SCANNERS

Physical print scanners, security devices that scan finger- or palm prints, carry Ratings of 1 to 6. Synthetic print duplications, which require a casting of the original print, carry a Rating of 1 through 4, depending on the technology used to make the phony print. The cost for the materials to manufacture a phony print is 200¥ per Rating Point. Characters must make a successful Intelligence Test against a Target Number of 3 in order to make an original cast good enough to create a usable phony print. The final product is a "sleeve" or glove-like membrane that fits over a wearer's hand.

Actual fingers or hands, removed from the owner, have a Rating of 8, but lose one Rating Point per hour after being removed from the original owner. Proper care of the appendage can slow the rating loss to one point per three hours. These guidelines also apply to the use of a finger or palm still attached to a dead person.

The finger or palm still attached to its living owner always works properly for a print scan.

A standard cost of 50,000¥ and Essence Rating loss of .1 are required to surgically implant retinal duplication of a Rating 1 retinal pattern. Each additional point of rating costs an additional 25,000¥, and so a Rating 4 duplication would cost 125,000¥. This cost is in addition to the standard cost of surgery. Essence cost is .1 for Rating 1 duplication, .25 for Ratings 2–4, and .5 for Ratings 5+. These Essence costs are in addition to the standard Essence costs required for surgery.

Retinal scanners are commonly available in Ratings from 3 to 9.

To use the print or retinal scanner systems, players must roll a number of dice equal to the rating of the print scanner against a target number equal to the rating of the phony print. If the scanner achieves at least 1 success in this test, it detects the fake and triggers a passive alert.

Characters can tamper with and defeat print scanners in the same way they can defeat cardreaders. See rules on p. 86.

VOICE RECOGNITION SYSTEMS

Unlike other scanner, or recognition, systems, voice recognition systems have an active component. These systems demand a response from an approved user's voice within a certain amount of time. If the response is not given within the time limit, the system sounds an alarm. These systems prove very difficult to tamper with physically because the security checkpoint requires only a simple microphone/speaker combination; the system's circuitry is secure in another part of the building.

Characters can only defeat voice recognition systems by speaking with the voice of an approved user, be it a recording, some other simulation, or the real voice.

Voice recognition systems carry Ratings of 1 to 10. The technology used to deceive these systems uses the same ratings scale. The Voice Technology Table lists the available voice reproduction technologies and their associated ratings and costs.

The voice modulator listed in the basic **Shadowrun** rules has a Rating of 1. Each additional point of rating added to this system raises the cost by 20,000¥, adds 1 to the Availability, and .1 to the Street Index. The maximum Rating available is 10.

In order to defeat a voice recognition system, the player must roll a number of dice equal to the recognition system's rating against a target number equal to the rating of the deception system. At the same time, the gamemaster rolls a number of dice equal to the deception system's rating against a target number equal to the recognition system's rating. The system that generates the most successes wins. Ties produce no results for either system, and the recognition system repeats its request for a response. The character may make another attempt to deceive the security system.

The voice mask system described in the **Street Samurai Catalog** cannot be used to deceive a voice recognition system. This system is designed to distort voices and cannot be used to replicate another voice.

VIBRATION DETECTORS

Runners may use their Stealth Skill to attempt to move undetected through an area protected by a vibration detector (if they know it's there, of course…). To determine success, make a Success Test each turn using the character's Stealth Skill against a target number equal to the vibration analysis software's rating. A single success means the character avoids detection for this turn. Unfortunately, the character may move only half a meter per turn when trying to avoid detection. Characters who want to move faster (1 meter per turn) must add +3 to the target number of the Stealth Test. Characters who move faster than one meter per turn automatically set off a vibration detector. Because vibration detectors pick up such low movement rates, defeating this type of system is difficult.

Typical analysis algorithms are Rated from 6 to 10+.

GAS DELIVERY SYSTEMS

Because timing is everything when determining the effectiveness of a gas-dispersal system, the gamemaster should use the following rules to determine how quickly the gas spreads, how quickly the characters notice it (if at all), and how quickly they can take action.

Dispersal systems like the Lethe system described on p. 59 can fill an area of 30 cubic meters in one Combat Turn (about 5 seconds). No simple way exists to determine *exactly* how quickly the gas spreads, but the following guidelines should serve in most cases. Gamemasters should feel free to make any on-the-spot modifications necessary.

The gas will spread at a rate of about 6 cubic meters (roughly 2 meters high, 2 meters wide, by 1.5 meters deep) every second. This takes up a varying number of Combat Turn phases. To determine the number of phases gas dispersal takes in each Combat Turn, divide the total number of phases in that Combat Turn (equal to the highest total Initiative rolled that turn) by 5. That number of phases equals approximately one second. For example, if Deathmask the street samurai rolls the highest Initiative that Combat Turn, a 25, one second would pass every 5 phases (25 ÷ 5).

The gas starts spreading during the Combat Phase in which the gas was triggered. If the dispersal lasts for multiple Combat Phases, the number of phases that constitutes one second may need to be recalculated. Characters who have actions remaining

VOICE TECHNOLOGY TABLE

Device	Rating	Cost	Availability	Street Index
Pocket Recorder (Cheap)	1	50¥	2/12 hrs	.75
Pocket Recorder (Expensive)	2	200¥	4/12 hrs	1
Portable Recorder (Basic)	3	900¥	4/36 hrs	1
Portable Recorder (Advanced)	4	1,600¥	6/72 hrs	1.5
Professional Deck (Basic)	5	25,000¥	8/7 days	1.5
Professional Deck (Advanced)	6	36,000¥	10/7 days	2

and are aware of the gas may take appropriate action. Characters who have Delayed Actions (p. 80, **SRII**) may make a Perception Test at the time of exposure to recognize the presence of the gas by rolling a number of dice equal to his or her Intelligence against a Target Number of 10, using the appropriate Perception Test modifiers from p. 185, **SRII**. Characters equipped with a gas spectrometer system (see **Shadowtech**, p. 61) modify their target number by −2.

Available portable gas detecting systems carry Ratings from 1 to 5 and cost their rating squared (Rating x Rating) times 5,000¥. They have an Availability of (Rating x 3) ÷ 7 days, and a Street Index of 2 (see **SRII**, p. 184–85 or **Shadowtech**, p. 101–102, for more information). Characters using portable gas detecting systems must roll a number of dice equal to the system's rating against a Target Number of 6 at the first exposure, and again for every additional second of exposure, adding −1 to the target number for each additional second of exposure. A gas detector exposed to gas for 3 seconds would have a Target Number of 4 (6 − 2). However, some gases are easier to detect than others. For example, the Neuro-Stun series is particularly difficult to detect, and the detection system receives no modifiers to detect these gases.

Characters wearing, or in the proximity of, a gas detector may make a Surprise Test (**SRII**, p. 86) to take appropriate action *if* they have a Delayed Action available (or act on that Combat Phase) and are receiving their initial exposure to the gas in the Combat Phase in which the gas detector alarm sounds.

Gases affect the body per the rules on page 186 of **Shadowrun, Second Edition**, or page 147 of the original **Shadowrun** rules. Updated versions of existing gas defenses and stats for the new gases mentioned on p. 19 appear below.

Neuro-Stun IX
Damage: 6S2-Stun {6S}   **Speed:** 1 turn
Description: Delivered as a gas in an organic binder, N-S IX takes effect if inhaled or upon contact with the skin. At the end of the turn in which a character is exposed to the gas, he suffers Stun damage. Even if he manages to resist this damage, he suffers disorientation for about an hour, adding +2 to all target numbers. The only difference between N-S IX and N-S VIII is the degree of persistence; N-S IX goes inert after 5 minutes. Neuro-Stun VIII becomes inert after 10 minutes.

Green Ring 3
Damage: 8S2 {8S}   **Speed:** 1 turn
Description: A nerve gas developed from research done in the 1970s, Green Ring 3 still shows characteristics of the gases "popular" during that time. It takes effect if inhaled or upon contact with the skin. At the end of the turn during which a character is exposed, he suffers 8S2 {8S} damage. Even if he manages to resist this damage, he or she suffers cramping, nausea, double vision, and crippling pain for one hour, which adds +5 to all target numbers for that time. Green Ring 3 persists for one hour, at the end of which time the gas has fully oxidized and become inert. It is, predictably, colorless and odorless.

Seven-7
Damage: 6D4 {10D}   **Speed:** 1 turn
Description: A cutting-edge war gas, Seven-7 hits sharp and hard, but persists for mere minutes. The gas takes effect if inhaled or upon contact with the skin, and will diffuse through standard chemsuits. Only military-issue "X-E" suits—15,000¥ each, in the unlikely event a character could get ahold of one—will block this diffusion. Standard chemsuits decrease the gas's dispersion speed to 2 turns.

At the end of the turn in which a character is exposed to the gas (or the end of the second turn, if he is wearing a chemsuit), he or she suffers the stated damage. Even if the character resists this damage, he or she suffers the same debilitating symptoms described for Green Ring 3 for a period of 6 hours and must add +5 to all target numbers for the duration.

Seven-7 oxidizes completely after 10 minutes, and is colorless and odorless.

Gamemaster's Note: We do not advocate making gas-based security systems standard within the game. As stated, they are difficult to detect and react to, and give players little or no chance to deal with a bad scene. Gamemasters should always try to provide the players with some sort of solution to a situation. No-win is no fun.

NETGUN SYSTEMS

In order for a netgun security system to be effective, the target must be in the weapon's preset line of fire. The chance of success depends on the skill of the person triggering the gun. (This rating represents the patience necessary to wait for the target to move into position, and the judgment needed to fire the gun at just the right moment.) Roll a number of dice equal to the operator's Willpower + Reaction divided by 3 (round fractions up). Note that firearms or other combat skills cannot be used to adjust this rating. The Target Number for this test is 6. (In the **Shadowrun, Second Edition** rules, the character triggering the system can only use dice from his or her Combat Pool.)

The netgun entangles its victim, restraining him and forcing him to the ground. The victim must make a Strength Resistance Test against twice the number of successes generated by the operator's success roll. The target can modify this test using his Dodge Pool, or the Combat Pool if using the **Shadowrun, Second Edition** rules. Once entangled, the victim is immobile and unable to act in any manner. The victim may attempt to escape from the net once per turn by making a Strength Resistance Test against a Target Number of 8, but must add a −1 modifier for every turn he or she has been entangled. The net receives 3 automatic successes against attempts to cut it. (**Shadowrun, Second Edition** rules do not allow automatic successes, and so increase the target number by 3.)

GUN SYSTEMS

Automatic gun systems come in two general types: "dumb" and "smart." Dumb weapons simply open up on an assigned area indiscriminately, much like an automatic sprinkler system. The objective of a dumb gun system is to fill the area with as much ammo as possible and hope to hit the target or targets. Systems of this nature are commonly used only in sealed areas with minimal chance of inflicting accidental or collateral damage. These systems usually fire Narcoject or stun rounds.

Dumb guns have a standard arc of fire, usually restricted to 180 degrees or less. Their accuracy depends on how much of the 180 degree arc they cover. Dumb guns covering a restricted 60 degree or less arc have an effective Firearms Rating of 4. Automatic guns covering 60 to 120 degrees have an effective Firearms Rating of 3, and those covering the full 180 degrees have a Rating of 2. These systems usually use the equivalent of an HK227 firing the appropriate round type at full autofire. The gun immediately attacks any target entering the assigned area of fire. If the target remains within the field of fire, he or she is attacked again every 10 Combat Phases. Automatic gun systems usually use rudimentary sensors that only indicate if a potential target is within the arc of fire. Standard dumb gun systems are activated by outside command and left to fire when a valid target appears.

In sharp contrast, smart guns, also referred to as autonomous gun systems, or sentry guns, use a selective system to choose targets. They selectively acquire and track targets and engage them with the appropriate rate of fire. Sentry systems (such as the recently trademarked Sentry™ line from Ares Arms) incorporate sophisticated low-light, thermographic, and ultrasound targeting and tracking systems into an advanced tactical analysis data processing system. Built around an assault rifle (FN HAR) or light machine gun (Ares MP-LMG) mechanism firing at minigun rates, these weapons fire in burst or autofire modes as appropriate (gamemaster discretion) and feed at least 1,000 rounds of ammunition. Traditionally mounted on tripods (providing 6 points of Recoil Compensation), these systems have 360 degree full-traverse mounting, allowing them to engage targets in any facing. Some systems include a vertical pivot system used to engage targets at up to a +20 degree inclination, or down to a –10 degree declination.

"Smart" automatic gun systems carry an effective Firearms Rating of 6 and have an Initiative of 25 + 2D6. The system will automatically delay actions (p. 80, **SRII**) as needed. As minigun-rate firing mechanisms, these systems can fire up to 15 rounds an action, usually in five 3-round bursts. They can and will engage multiple targets within one action.

Advanced systems like the Ares Sentry™ models incorporate a microtronic version of the tactical computer described in **Shadowtech**, p. 53. These systems have an effective Intelligence of 8, and so can "mark" and track up to eight separate targets.

DOOR/WINDOW ALARMS

With the right tools, characters may almost routinely defeat a simple door or window alarm. Getting past the alarm requires two steps. First, the character must make a Perception Test against a Target Number of 3 to determine the location of the alarm contacts. The character may choose instead to use his or her Electronics Skill or a suitable Concentration/Specialization, but must then use Target Number 5. On 1 success, the character locates the alarm contacts.

Once the contacts have been located, in order to defeat the system the player makes an Electronics Test against a Target Number of 4 or higher, at the gamemaster's discretion (the better the security system, the higher the target number). Use the modifiers suggested in the Build/Repair Skill Situational Modifiers Table, p. 154, **Shadowrun**, or apply the modifiers from the Build/Repair Table on p. 183, **Shadowrun, Second Edition**.

LASER SYSTEMS

The two-step laser system described on p. 17 can deliver a pulse of energy inflicting up to 10S2 {**10S**} damage.

ELECTRIC FENCES

A character who touches a charged electric fence takes damage as from a shock weapon (see **Shadowrun**, p. 120, or **Shadowrun, Second Edition**, p. 103), 4D2 Stun {or **4D** using the **SRII** rules}. The character must also make a Willpower or Body Test against a Target Number of 4 to remove his or her paralyzed hands from the fence. Failure to achieve any successes means that the character remains in contact with the fence and receives another 4D2 Stun {**4D**} attack in 10 Combat Phases. If knocked unconscious by the damage, the character receives one, final 4D2 {**4D**} shock before his muscles go slack and he drops to the ground. Regardless of how many shocks the character receives or when he goes unconscious, he still suffers the long-term stun effects of the shock.

Any shock-type damage the character takes may also damage his or her cyberware. See **Street Samurai Catalog**, pp. 93–95, or **Shadowtech**, p. 39, for more information.

MONOWIRE

To spot a trap consisting of taut monowire, a character must make a successful Perception Test against a Target Number of 6. Apply the visibility modifiers from the Visibility Table, p. 66, **Shadowrun**, or p. 89, **Shadowrun, Second Edition**, in addition to the following modifiers:

ADDITIONAL VISIBILITY MODIFIERS TABLE	
Situation	**Modifier**
Character distracted/running	+2
Illumination level changing	Add +1 to modifier of worst level

Characters that run into a monowire take 7S4 {**11S**} damage. If walking, the character takes only 5S4 {**9S**} damage. A character who grabs a strand of monowire is subject to 4S3 {**7S**} damage. Impact armor offers one-half (round down) protection against this damage. Dodge Pool dice (or Combat Pool dice, **SRII**) do not help in making the Damage Resistance Test.

SECURITY GUARDS

The security personnel levels provided in this book reflect the Professional and Threat Rating systems described on p. 187, **Shadowrun, Second Edition**. The numbers translate as follows:

Personnel Quality	Professional Rating	Threat Rating
A	3	3
B	2	2
C	1	2

PLANES AND CREWS

The following vehicle and character archetypes represent typical planes and their crew members.
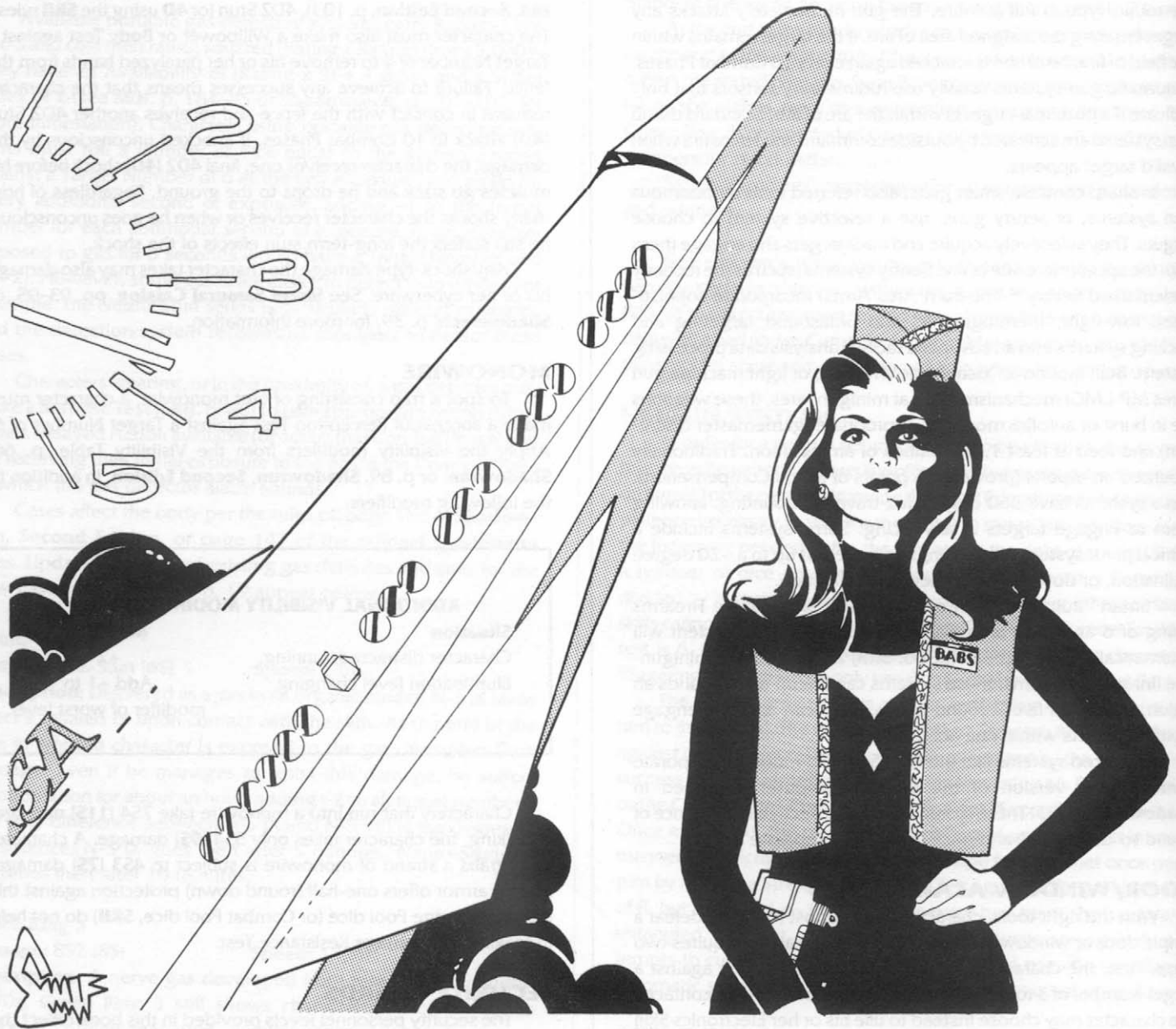
GENERAL DYNAMICS SV250 SEMIBALLISTIC

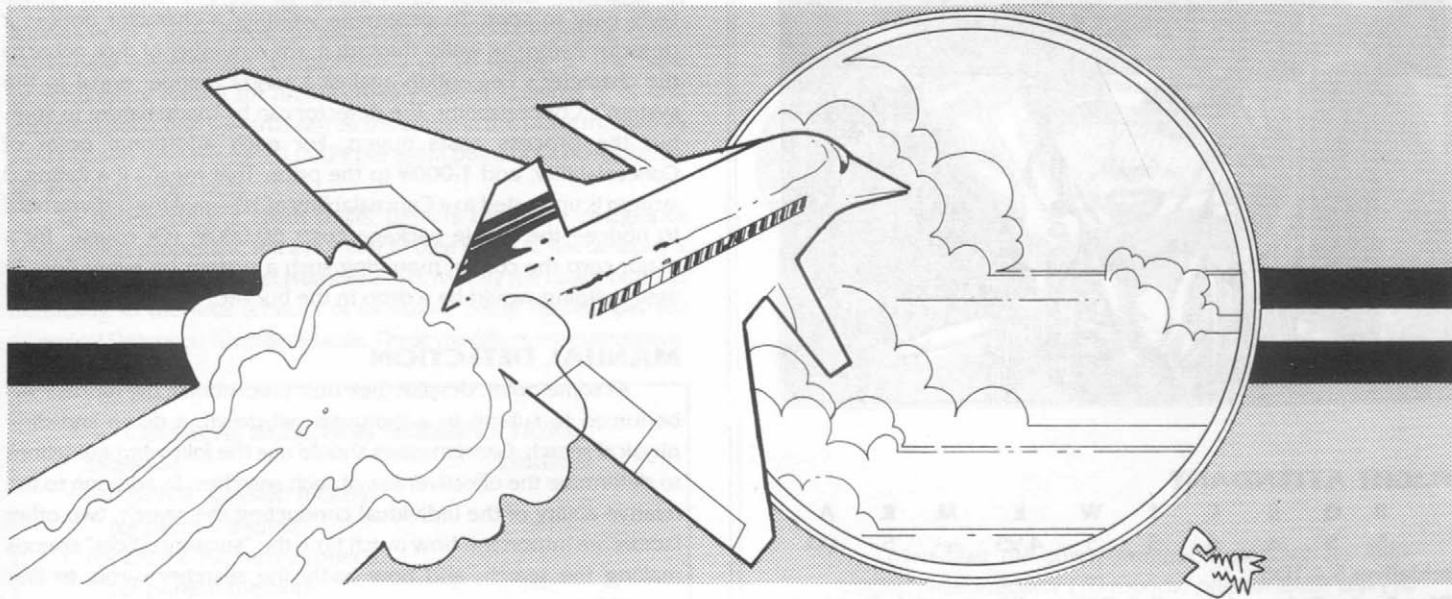| Handling	Speed	Body	Armor	Sig	APilot	Cost
6	10,000/29,000	5	2 (6)	1	4	750 million ¥

Semiballistics have a minimum air speed of 250 kph. They require a flight deck crew of two and carry 150 passengers. Four to eight crew work in the cabin, depending on the carrier. The vehicle measures almost 110 meters long, has a wingspan of about 35 meters, and masses about 300,000 kilograms. All planes of this type carry cybernetic vehicle control systems and minimal manual controls as standard equipment.
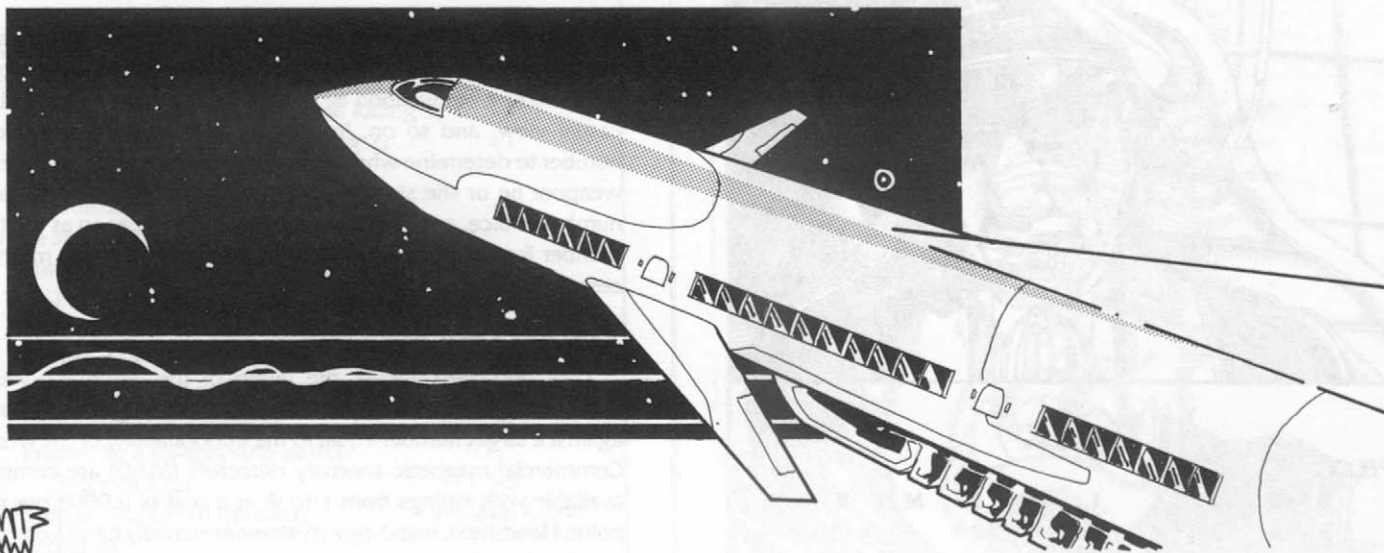
"CHINA CLIPPER" SUBORBITAL

Handling	Speed	Body	Armor	Sig	APilot	Cost
5	10,000/24,000	5	2 (6)	1	3	100 million ¥

Suborbitals have a minimum air speed of 200 kph. They require the same number of crew and carry as many passengers as semiballistics, and have similar exterior dimensions. All planes of this type carry cybernetic vehicle control systems and minimal manual controls as standard equipment.

"ARROW" HSCT

Handling	Speed	Body	Armor	Sig	APilot	Cost
5	1,500/2,900	4	1 (3)	2	4	10 million ¥

HSCTs have a minimum air speed of 100 kph. They require the same flight deck crew as the semiballistic and suborbital planes, but can carry up to 300 passengers. The HSCT is 95 meters long, has a wingspan of 40 meters, and masses about 335,000 kilograms. All planes of this type carry cybernetic vehicle control systems and minimal manual controls as standard equipment.

PILOT

B	Q	S	C	I	W	E	M	R	A
3	4	3	4	4	4	2	—	4 (8*)	—

Initiative: 4 (8 when rigging) + 1D6 (3D6 when rigging)
Dice Pools: Defense (Armed) 1, Defense (Unarmed) 1, Dodge 4
{**Threat/Professional Rating: 2/2**}
Skills: Etiquette (Corporate) 3, Physical Sciences (Aerodynamics) 3, Winged Planes (B/R) 3, Winged Planes 8 (Jets 4)
Cyberware: Vehicle Control Rig (2)
*Only when rigging.

FLIGHT ATTENDANT

B	Q	S	C	I	W	E	M	R	A
5	5	4	4	5	5	4.95	—	5	3/0

Initiative: 5 + 1D6
Dice Pools: Defense (Armed) 1, Defense (Unarmed) 1, Dodge 4
{**Threat/Professional Rating: 3/3**}
Skills: Armed Combat 5, Etiquette (Corporate) 4, Firearms 6, Firearms (Tasers) 4, Leadership 3, Negotiation 3, Psychology 2, Unarmed Combat 6
Cyberware: Datajack, Display Link, Headware Radio
Gear: Armored Clothing, Concealed Knife, Shock Gloves or Stun Baton, Taser

WEAPON DETECTION

Shadowrun weapons use a Concealability Rating. This single number incorporates several factors: weapon size, how bulky and cumbersome the weapon is, how easily it can be concealed from casual view, and so on. In general, gamemasters can use this number to determine whether or not a metal detector registers the weapon: he or she simply uses the rating of the detector as the number of dice, and the Concealability of the weapon as the target number for the test. If the gamemaster achieves 1 or more successes, the weapon has been detected.

AUTOMATIC SYSTEMS

As described above, the rating of the automatic weapon detection system is used as the base number of dice to be rolled against a target number equal to the Concealability of the weapon. Commercial magnetic anomaly detectors (MAD) are commonly available with Ratings from 1 to 9, at a cost of 5,000¥ per rating point. Hand-held, wand-type systems are usually rated from 1 to 4, and free-standing or architecturally mounted systems are rated at 3 or better.

Gamemasters may decide to make their game a little more complex. Because some weapons described in the **Street Samurai Catalog** have casings of macroplast and other non-metallic materials, like the Glock described on p. 57, these weapons contain less metal, and should logically be more difficult to detect. Gamemasters can add +1 or +2 to these weapons' Concealability against metal detectors *only*.

A standard detector has a Concealability Rating of 5, making it fairly easy to spot. To determine whether a character notices a detector *before* he walks through it, roll a number of dice equal to the character's Perception against a target number equal to the system's Concealability. The detector can be made harder to spot, but the process costs nuyen. For each additional point of Concealability, add 1,000¥ to the price. That means if a Rating 8 system is upgraded to a Concealability of 10—making it *damn* hard to notice—the whole package costs 50,000¥. (Of course, for a major corp the cost of mounting such a system on every door in their building would be a drop in the bucket.)

MANUAL DETECTION

At some point, despite their best precautions, the runners will be forced to submit to a thorough pat-down, a down-and-dirty physical search. Gamemasters should use the following guidelines to determine the effectiveness of such searches. In addition to the relative ability of the individual conducting the search, two other factors are important: how much time the "security officer" spends making the search, and how badly the searcher wants to find something.

In all cases, make a standard Perception Test against the Concealability of the weapon in question. (Roll a number of dice equal to the searcher's Intelligence against a target number equal to the Concealability of the weapon.) Apply the modifiers in the Manual Detection Modifiers Table.

MANUAL DETECTION MODIFIERS TABLE

Situation	Modifier
Searcher's level of professionalism:	
Average/Amateur (Professional Rating 1)*	+2
Semi-trained (Professional Rating 2)*	+1
Trained or better	
(Professional Rating 3 or 4)*	+0
Time spent on the search:	
Cursory (very quick pat-down)	
(1–2 seconds)	+2
Brisk (fast pat-down) (3–5 seconds)	+1
Standard (6–20 seconds)	+0
Detailed (21–60 seconds)	−1
Deliberate (1–2 minutes)	−2
Practically a fraggin strip search	
(3–5 minutes)	−3
Strip search (6–10 minutes)	Weapon found
Searcher is:	
Intimidated/Fearful	+2
Working under normal conditions	+0
In complete control	−2

*Refers to the Professional Rating rules in **Shadowrun, Second Edition**, p. 187

CHEMICAL DETECTION SYSTEMS

Chemical detection systems appear more rarely than MAD-based systems, but are generally more effective. Available in Ratings from 1 to 8, these systems cost 70,000¥ per Rating Point. Hand-held systems are available only up to Rating 3. The base Concealability Rating for architecturally based systems is 4, and chemical detection systems can be modified in the same manner as MAD-based systems for 25,000¥ per extra point of Concealability, up to a maximum of 8.

To determine if a chem-sniffer detects explosive charges or ammunition propellant, roll a number of dice equal to the detector's rating against a Base Target Number of 10. Modify the target number according to the total amount of explosive being carried, per the Chemical Detection Modifiers Table. These modifiers are cumulative.

CHEMICAL DETECTION MODIFIERS TABLE

Situation	Modifier
For each 8 standard rounds	
(or portion thereof)	−1
For each 6 explosive rounds	
(or portion thereof)	−1
For each 1 concussion or	
fragmentation hand grenade	−1
For each 2 smoke or flash grenades	−1
For each 3 mini-grenades (any type)	−1
For each 30 grams of standard	
(non-plastique) explosive	−1
For each 100 grams of plastique	−1

Mau-Mau the street samurai is packing his fully-loaded Ares Predator (10 rounds) plus an extra clip (10 rounds), and two frag grenades. Blissfully ignorant of the risk, he wanders through a chem-sniffer in the MCT skyraker. Twenty rounds of non-explosive ammo modifies the Detection Test target number by −3. Two grenades provide an additional modifier of −2, for a total modifier of −5. The Base Target Number for a chem-sniffer is 10, and so the modified Target Number is only 5. Odds are, Mau-Mau's in deep drek.

LAUPENSTEIN·92

ARMOR CLOTHING

These items of clothing represent a new wave in armored apparel—protection without detection. They are designed to give the wearer the appearance of complete vulnerability while providing a defense against the unexpected.

When combining pieces of armored clothing such as those in the Vashon Island line, add the ratings of each piece being worn together and round the total down. A complete "Houndstooth" set would have a Ballistic Rating of 3 and an Impact Rating of 3.

The Availability and Street Index of all items in the Armor Clothing Table is as follows: the target number for Availability is equal to the combined Ballistic and Impact ratings, and the base time is 48 hours. The Street Index is .75.

LAYERING ARMOR

It is possible to layer armor, but even layered armor has limited effect. When layering armor, add the rating of the highest-rated piece to one-half (round down) the rating of the next highest-rated piece of clothing or armor to determine the effective combined value. Generally, only a jacket or coat can be layered over clothing-style armor.

ARMOR AND SOCIETY

So what kind of reaction can a character expect if he or she is déclassé enough to wear his or her armor to dinner?

The glitterati of the city will react negatively, with scornful looks, or obvious cold shoulders. In general, if a *shaikujin* or corp executive who lives the Luxury lifestyle (**Shadowrun**, p. 148, or **SRII**, p. 189) spots a character's armor, add a +2 modifier to the character's target number for using a non-abusive Social Skill. ("Non-abusive" in this case means attempts to fast-talk, befriend, con, seduce, or otherwise influence a target.) On the other hand, visible armor gives the character a –1 modifier to his or her target number for intimidating these people…

Many luxury-class establishments will simply deny entry to a character wearing noticeable armor. (Such places are likely to use detectors more sensitive than the doorman's eyes.) Most high-class establishments will not try to keep out obviously armored characters, but the bouncers may pay the character such an inordinate amount of attention that his or her stay becomes very uncomfortable. These bouncers will stand ready to wade in and stop any trouble in which the characters get involved.

As Zeppo mentioned on page 38, even some lower-class establishments are starting to come down heavy on armor, and may even go so far as to deny an armored character entry.

The gamemaster should keep this new attitude in mind, and make a lot of Perception/Intelligence rolls to determine if "polite" society spots the runners' heavy armor. Make enough rolls to convince the runners to change their ways, or just make them nervous enough to reconsider their personal style when running biz.

ARMOR CLOTHING TABLE

|	Concealability	Ballistic	Impact	Weight	Cost
Armanté					
"Venetian" dress	14	1	0	.5	3,500¥
"Starlight" dress	13	1	1	.75	4,500¥
"*Ancien*" shawl	14	1	0	.3	750¥
"Executive Suite" tuxedo	12	3	1	1	1,100¥
"London Fog" cloak	12	2	2	1	600¥
Mortimer of London					
"Greatcoat"	11	4	2	3	1,000¥
Vashon Island					
"Houndstooth" suit jacket	14	1.5	.5	1	*
"Houndstooth" pants	14	1	.5	1	*
"Houndstooth" suit vest	13	.5	1	.75	*
"Houndstooth" sports jacket	12	.5	1.5	1.25	*
"Hunt Ball" jacket	13	.5	1.5	1	**
"Hunt Ball" skirt	14	.5	1	1	**
"Hunt Ball" slacks	14	1	.5	1	**
Zoé					
"Retrovision" skirt suit	13	3	1	1.5	2,500¥
"Country Club" blazer	13	3	1	1	2,000¥
"Highland Laird" kilt	14	4	2	1.5	2,000¥

*The "Houndstooth" collection is available as a package only and costs 2,000¥.

**The "Hunt Ball" collection is available as a package only and costs 3,000¥.

DOCWAGON

DocWagon created a whole new way to look at health-care service. Their innovations touched every aspect of emergency treatment, including the emergency vehicle and personnel training. The following new vehicle and NPC Archetypes can be used to respond to DocWagon™ calls during an adventure. Additional information on the DocWagon system appears following these stats.
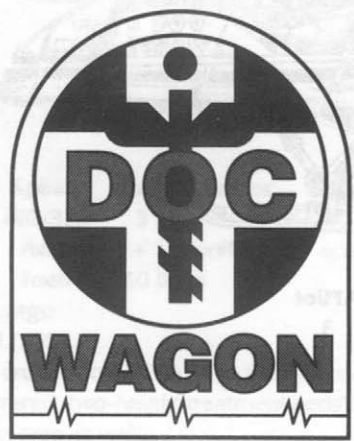
STANDARD RESPONSE TEAM

Personnel

B	Q	S	C	I	W	E	M	R	A
3	4	3	3	4	3	6 (5.5*)	—	4	5/3

Initiative: 4 + 1D6

Dice Pools: Defense (Armed) 1, Defense (Unarmed) 2, Dodge 4

**{Threat/Professional Rating: 2/2}**

Skills: Biotech 5, Car 3, Cybertechnology 1, Firearms 2, Unarmed Combat 2

Cyberware: None (or datajack*)

Gear: Armor Jacket (5/3), Fichetti Security 500 [Light Pistol, 25 (clip) {SA}, firing gel rounds at 4L1 Stun {4L Stun}, w/two extra clips], (1) Flash Grenade, Medkit, Slap Patches (5 of each type, Rating 3), (1) Smoke Grenade

Vehicle carries one Defiance T-250 shotgun [Shotgun, 5 (mag) {SA}, firing gel rounds at 3M2 Stun {9S Stun}, w/10 extra rounds]
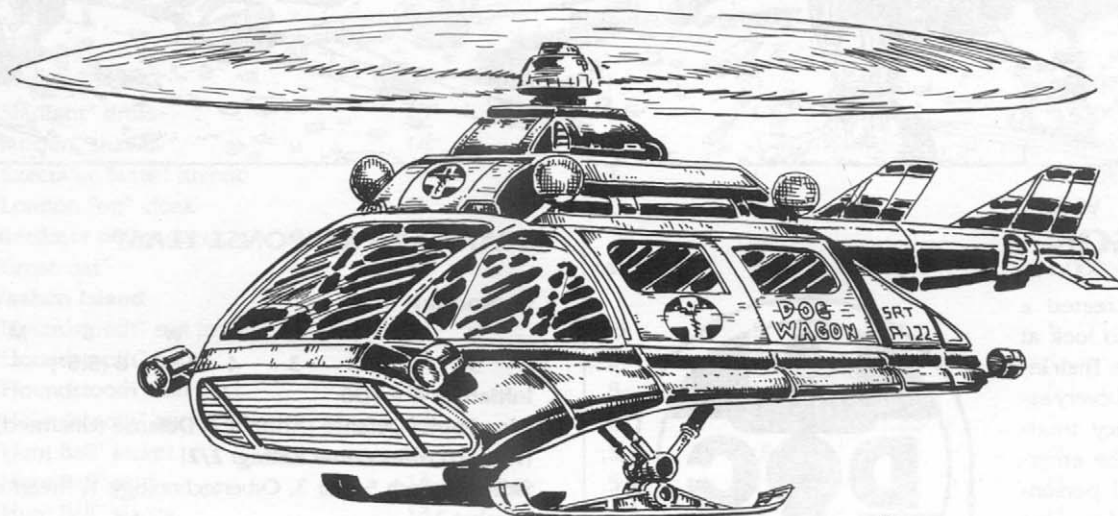
*Ambulance driver only
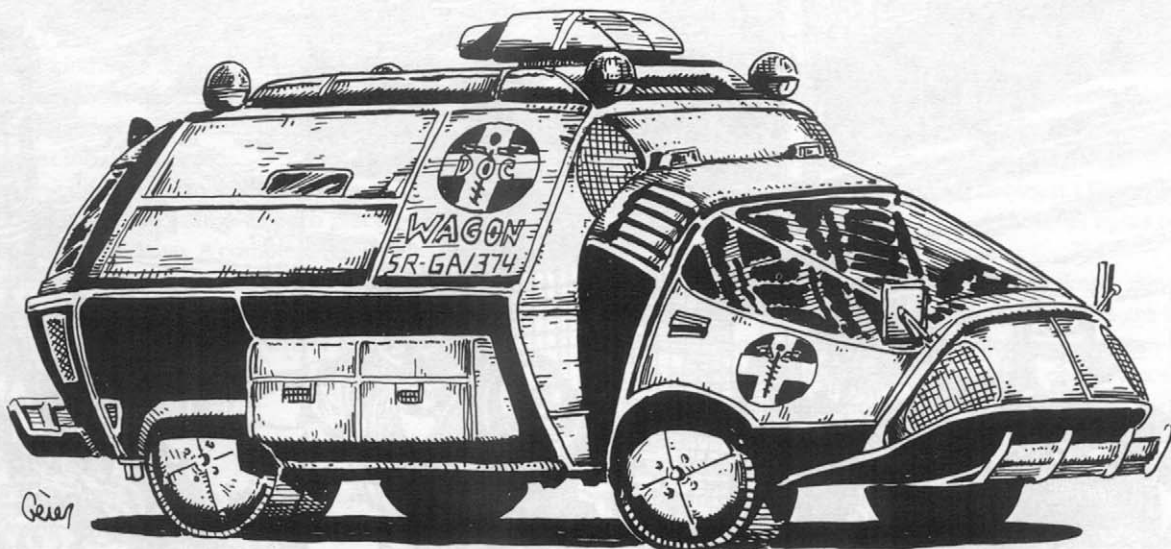
Vehicles

SRT Ground Ambulance

	Handling	Speed	Body	Armor	Signature	APilot
SRT Ambulance	4/10	30/75	4	0	2	1

Seating: Twin bucket seats   **Access:** 2 standard + double rear
Economy: 16 km per liter   **Fuel:** IC/80 liters
Cargo: 6 CF in assorted stowage lockers
Additional Features: Rear area is inaccessible from the driver compartment and contains the medical gear and single-patient treatment area (usually taken up by a wheeled gurney). Cramped space is available for one medical attendant and one additional passenger in this area as well.

SRT Helicopter

	Handling	Speed	Body	Armor	Signature	APilot
SRT Helicopter	5	170/250	4	0	4	3

Seating: Twin bucket seats   **Access:** 2 standard + 1 double sized
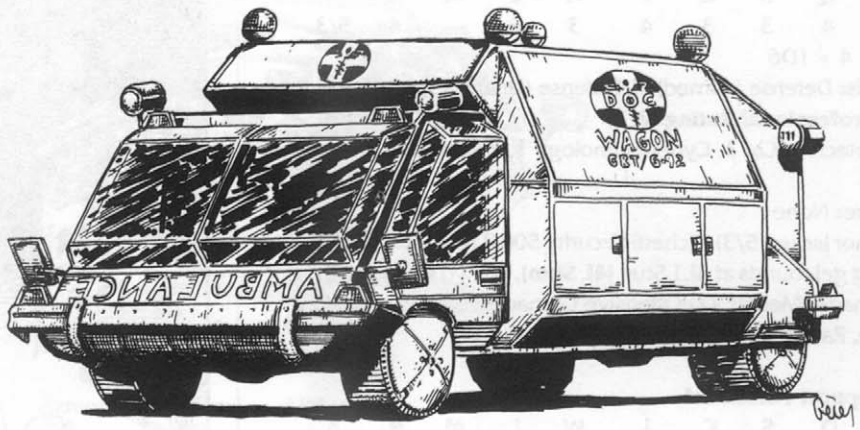**Economy:** .25 km per liter   **Fuel:** IC/1,250 liters
Cargo: 4 CF in stowage compartments
Additional Features: The rear area contains gear similar to the standard SRT ground ambulance, but can only accommodate the medical equipment, the patient, and one medical technician.

CRISIS RESPONSE TEAM

Personnel

Use the personnel stats provided for the Standard Response Team. Both response teams carry members with identical training.

Vehicles

CRT Ground Unit

	Handling	Speed	Body	Armor	Signature	APilot
CRT Ambulance	4/10	30/75	5	0	2	2

Seating: Twin bucket seats   **Access:** 2 standard + double rear
Economy: 12 km per liter   **Fuel:** IC/100 liters
Cargo: 8 CF in assorted stowage lockers

Additional Features: Rear area is inaccessible from the driver compartment and contains medical gear and a four-patient treatment area (usually configured as double-deck style treatment beds on each side of the vehicle). Sufficient, though cramped, space is available for six medical attendants but no passengers.
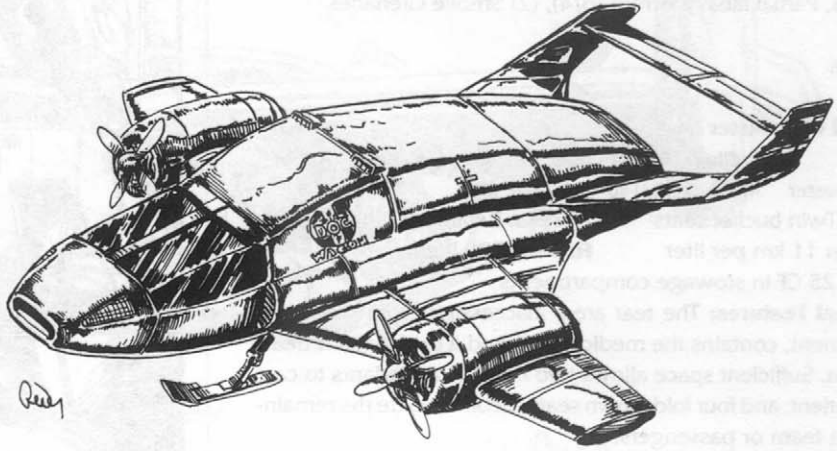
CRT Air Unit

	Handling	Speed	Body	Armor	Signature	APilot
CRT Tilt-Rotor	5	140/320	3	0	3	3

Seating: Twin bucket seats   **Access:** 1 + 1 modified rear access
Economy: 2.5 km per liter*   **Fuel:** IC/750 liters
Cargo: 10 CF storage + 15 CF cargo
Landing/Takeoff Profile: VTOL/STOL

Additional Features: The rear area, inaccessible from the driver compartment, contains the medical gear and a four-patient treatment area (usually arranged into two staggered, two-height treatment beds). Sufficient, though cramped, space is available for six medical attendants and one additional passenger in this area as well.
*VTOL Economy .5 km/liter

HIGH THREAT RESPONSE TEAM

Personnel

Medical Personnel

B	Q	S	C	I	W	E	M	R	A
3	4	3	3	4	3	6	—	4	5/3

Initiative: 4 + 1D6
Dice Pools: Defense (Armed) 1, Defense (Unarmed) 3, Dodge 4
{Threat/Professional Rating: 2/3}
Skills: Biotech 5, Car 3, Cybertechnology 1, Firearms 3, Unarmed Combat 3
Cyberware: None
Gear: Armor Jacket (5/3), Fichetti Security 500 [Light Pistol, 25 (clip) {SA}, firing gel rounds at 4L1 Stun {4L Stun}, w/two extra clips], (1) Flash Grenade, Medkit, (2) Offensive Grenades, Slap Patches (5 of each type, Rating 3), (1) Smoke Grenade

Threat Support Personnel

B	Q	S	C	I	W	E	M	R	A
4	5	4	2	3	4	.1	—	4 (8)	6/4

Initiative: 4 (8) + 3D6
Dice Pools: Defense (Armed) 3, Defense (Unarmed) 4, Dodge 4
{Threat/Professional Rating: 4/3}
Skills: Armed Combat 3, Biotech 1, Car 4, Firearms 6, Gunnery 2, Unarmed Combat 4
Cyberware: Cybereyes with Low Light, Smartlink, Wired Reflexes (2)
Gear: (1) Concussion Grenade, (2) Flash Grenades, (1) Gas Grenade, H&K 227-S [SMG, 28 (clip) {SA/BF/FA}, 5M3 {7M}, Internal Smartgun, Gas-Vent (3)], Medkit, Micro-Transceiver, (2) Offensive Grenades, Partial Heavy Armor (6/4), (2) Smoke Grenades

Vehicles

Modified Citymaster

	Handling	Speed	Body	Armor	Signature	APilot
HTR Citymaster	4/10	35/140	4	2 {6}	2	3

Seating: Twin bucket seats   **Access:** 2 standard + 1 rear hatch
Economy: 11 km per liter   **Fuel:** IC/500 liters
Storage: 25 CF in stowage compartments
Additional Features: The rear area, inaccessible from the driver compartment, contains the medical gear and a dual-patient treatment area. Sufficient space allows two medical attendants to care for the patient, and four fold-down seats accommodate the remainder of the team or passengers.

The turret, operable from the driver area, mounts twin light machine guns [LMG, 1,000 rounds {FA}, 4M4 Stun {5S Stun}]. Use one-half recoil modifiers because of the hardpoint mounting.

Geier

Modified Hughes WK-2 Stallion

	Handling	Speed	Body	Armor	Signature	APilot
HTR Helicopter	5	165/235	5	2 (6)	4	3

Seating: Twin bucket seats   **Access:** 2 standard + double sized

Economy: .23 km per liter   **Fuel:** IC/1,250 liters

Cargo: 2 CF in assorted stowage lockers

Additional Features: The rear area contains gear similar to the standard SRT ground ambulance, but provides only enough space for the medical equipment, the patient, and one medical technician.

The vehicle mounts two hardpoints, usually fitted with M107 GPHMGs [HMG, 1,000 rounds {FA}, 6M4 Stun {8S Stun}], though other weapons can be mounted to meet specific needs.

Osprey II

	Handling	Speed	Body	Armor	Signature	APilot
HTR Osprey II	5	190/380	3	1 (3)	2	3

Seating: Twin bucket seats   **Access:** 1 + 1 modified rear access

Economy: 3 km per liter*   **Fuel:** IC/600 liters

Cargo: 6 CF storage + 6 CF cargo

Landing/Takeoff Profile: VTOL/STOL

Additional Features: The rear area, inaccessible from the driver compartment, contains medical gear and the two-patient treatment area. Sufficient, though cramped, space exists for two medical attendants and three fold-down seats for the remaining team members or passengers.

The vehicle mounts two hardpoints, usually fitted with M107 GPHMGs [HMG, 1,000 rounds {FA}, 6M4 Stun {8S Stun}], though other weapons can be mounted to meet specific needs.

*VTOL Economy 1 km/liter

DOCWAGON VEHICLE SECURITY

All DocWagon vehicles are designed so that the patient compartment is separate from the driver's or pilot's compartment. When DocWagon personnel leave their vehicle unattended, they lock all doors with built-in maglocks.

The patient compartment is secured with a thumbprint scanner (Rating 5), and a Rating 6 palmprint scanner secures the driver's compartment. Built "smart" enough to detect if the owner of the thumb or palm is dead (but not unconscious), or if the extremity is no longer attached to its owner, the lock will not open to attempts under these circumstances.

If a character attempts to bypass one of these locks and fails, the system automatically transmits a warning to the transceivers worn by the DocWagon team to inform them that their vehicle is under attack. The team's response depends on the circumstances, but almost all HTR teams take violent exception to such attempts.

DOCWAGON CLINICS

For the layout of a typical DocWagon clinic, use the Hospital Archetype from **Sprawl Sites**. Supplement the hospital personnel with 4D6 standard DocWagon medical personnel and 2D6 threat support personnel.

RESPONSE TIME

The following guidelines represent average DocWagon response times to a specific call. The examples given apply to Seattle, though DocWagon response teams in virtually any city will face similar situations.

Seattle's DocWagon coverage is provided by one franchise, though some large cities may have multiple franchises. Two factors determine response time: the availability of ground or air units, and the physical location and Enforcement Rating of the area from which the call originated. Obviously, the further away the available unit, or the more dangerous the area, the slower response time will be.

When DocWagon receives a call for assistance, the gamemaster must first determine the type of unit available to respond by rolling 1D6. On a result of 1–4, the responding DocWagon vehicle is a ground vehicle of the appropriate type. On a result of 5–6, it is an air vehicle of the appropriate type. HTR units will respond to an appropriate call with a ground vehicle on a result of 1–3, and an air unit on a 4–5 (Stallion) or 6 (Osprey II).

To determine the response time, roll 3D6 and modify the result using the DocWagon Response Time Table. Apply all applicable modifiers, which are cumulative. The response time will always be at least four minutes.

DOCWAGON RESPONSE TIME TABLE

Situation	Modifier
Area:	
Auburn	+1
Bellevue	—
Council Island	–1
Downtown	–1
Everett	+2
Fort Lewis	+2
Puyallup	+2
Redmond	+1
Renton	—
Seattle proper	–1
Snohomish	+1
Tacoma	+1
Salish-Shidhe Council Lands	*
East of the city	+3
West of the city	+3
North of the city	+5
South of the city	+5
Farther than 10 miles	
beyond the border	+2
Farther than 25 miles	
beyond the border	NA
Corporate-owned territory	**
Enforcement Rating	
AAA–AA	–2
A–B	–1
C	—
D	+1
E	+2
Z†	+3
Type of Response	
Standard Response Team	—
Critical Response Team	+1
High Threat Response	***
Ground Vehicle responding	—
Air Vehicle responding	–2

*DocWagon Seattle made a special arrangement with the Salish-Shidhe Council for emergency response into S-S Council lands. DocWagon may not contract their services within S-S Council lands, but can respond to calls from Seattle clients within 25 miles of the Seattle Metroplex border. Calls made from beyond the 25-mile limit cannot be answered. The agreement with the Council requires that all DocWagon patients except for those in extreme trauma must be delivered to the nearest health-care facility, especially if such a facility is within the S-S Council lands. (This guarantees that DocWagon will spend the shortest amount of time possible in Council lands, and often produces revenue for the Council for providing treatment.) The ten-minute-response service clause is automatically waived for any assistance required in Salish-Shidhe territory.

**DocWagon will not respond to calls made from extra-territorial corporate territory, or any grounds belonging to a foreign government, or the UCAS government, without first obtaining express permission from that corporation or government. Normally, this means that if the call involves action against said corporation or government, service will be denied unless that corporation or government is feeling particularly benevolent, or (more likely) the response is somehow to their advantage. Obtaining extra-national permission usually increases the base response time by 4D6. The gamemaster makes the final call in all matters of extraction from extra-national territories and permission to provide service in these areas.

***If dispatched immediately upon receiving a call, the response time for a High Threat Response team is modified by –1. If a Standard Response Team responds to a call and then calls for HTR back-up, the response time is calculated normally. The ten-minute-response service clause is waived in such cases.

†The ten-minute-response clause is automatically void for calls originating in an Enforcement Rating Z area.

HELP (ALMOST) TOO LATE

Whether or not DocWagon will pick up the tab if they arrive late on the scene depends upon the existence of any extenuating circumstances. To determine whether DocWagon will consider the circumstances surrounding their response standard or unusual, roll 2D6. Under standard circumstances, DocWagon will provide free care if the die roll result is 10 or less. In a less-than-ideal situation, they may decide that their response was slowed by circumstances beyond their control. Apply the appropriate modifiers from the DocWagon Loophole Table to a Base Target Number of 10 to find the modified target number, then roll 2D6. If the result is greater than the modified target number, DocWagon has found a legal contractual "out" that invalidates the ten-minute-response clause.

DOCWAGON LOOPHOLE TABLE

Situation	Modifier
Unusual social disturbances	–4
Excessive number of service calls	
simultaneously	–4
Customer involved in an active	
combat situation	–2
Enforcement Rating E area	–2
HTR called for by SRT	Clause waived

COFFIN HOTELS

Coffin hotels offer a cheap, convenient, relatively comfortable, and surprisingly secure place to spend the night or lay low.

COFFIN SECURITY

Coffin hotel cubicles are usually secured by Rating 5 print-scan maglocks. The central computer system controlling the locks is protected by defenses consisting of Orange-4 with Blaster 3 and Trace and Dump 4. (This level of IC is not heavy enough to protect the clients, but is designed to prevent smart guys from defrauding the system.)

Any alert triggered by the computer summons the manager on duty plus one or more security guards, depending on the nature of the alert. For the manager, use the Bartender Contact, p. 163, **SR**, or p. 203, **SRII**, with Etiquette (Street) 4, Firearms 2, Unarmed Combat 2, and Special Skill of Hotel Management 3. For the security guards, use the Corporate Security Guard Contact, p. 165, **SR**, or p. 205, **SRII**.

At any given time, an average coffin hotel has 2D6 x 10 patrons in residence. Most patrons are Low-lifestyle street types, but one or more shadowrunners or other individuals may be renting a space in order to keep a low profile.

The coffin itself provides a Barrier Rating of 12 to those inside.

MCHUGH'S

The fast-food restaurant well known in the sprawl for its high level of customer safety, if not for daily epicurean delights, McHugh's provides an excellent example of the latest trend in inexpensive dining establishments. The following information can easily be applied to any other similar-sized restaurant. Gamemasters should feel free to adapt these employees and facilities as needed.

ARCHETYPES

Manager: Use Bartender, p. 163, **SR**, or p. 203, **SRII**, with Etiquette (Corporate) 3, Etiquette (Street) 3, Special Skill of Street Rumormill 1. He keeps an Ares Slivergun in the top right-hand drawer of his desk.

Bus Staff: Use Pedestrian, p. 116, **Sprawl Sites**, or p. 25 of the **Contacts Book** included in the **Shadowrun Second Edition Gamemaster's Screen (SRIIGM)**.

Cook: Use Pedestrian, p. 116, **Sprawl Sites**, or p. 25 of the **Contacts Book/SRIIGM**, with Food Preparation 1. (He or she watches the machines to make sure nothing goes wrong.)

Typical Patron: Anyone with a couple of nuyen, but frequently families.

NUMBER OF PEOPLE PRESENT

1 Manager, 3 Bus Staff, 2 Cooks, 6 Security Guards (see below), 3D6 – 3 Patrons.

COMPUTER

Green-4, Barrier 4. Functions limited to storing information on current sales and inventory. McHugh's keeps all personnel records at their corporate headquarters.

MCHUGH'S SECURITY PERSONNEL

B	Q	S	C	I	W	E	R	Armor
5	5	4	3	3	3	5.1	4	5/3

Initiative: 4 + 2D6
Dice Pools: Defense (Armed) 1, Defense (Unarmed) 2, Dodge 5
[Threat/Professional Rating: 3]
Skills: Etiquette (Corporate) 4, Etiquette (Street) 2, Firearms 5, Interrogation 2, Unarmed Combat 4
Cyberware: Air Filtration System (4), Boosted Reflexes (1)
Gear: Armor Jacket (5/3), Browning Max-Power (w/extra clip), Defiance Super Shock Taser, Micro-Transceiver, Shock Gloves (see **Street Samurai Catalog**, p. 11)

PHYSICAL SECURITY

The door frame contains a Rating 5 metal detector and a Rating 4 chem-sniffer. For detection purposes, consider the two systems as one with a Concealability of 3. The rear door locks with a Rating 5 keypad maglock.

FORGING CREDSTICKS AND IDS

Forging a credstick is a difficult task. Though the stick itself may be easy enough to rig, fabricating the background identification files that make a credstick legitimate requires considerable effort.

In a credstick ID verification, the information offered by the credstick is instantly cross-referenced and double-verified through a dozen or more channels. Such cross-referencing is a simple matter for the international computer grid of the Matrix, and so falsifying an identity involves an incredible amount of electronic manipulation. That is, someone must create and covertly insert into the world's data banks a suitable, appropriate, and credible "credit history" that appears to be a permanent part of the information net.

An average Joe working at home on his legal cyberdeck has no hope of creating a usable false ID for a credstick. Only an expert and a well-connected expert at that, possesses the resources to pull off a scam of these proportions. Entire shadowy organizations exist solely for the purpose of creating false identities and credsticks. These organizations, normally based in one of the world's data havens, maintain contact with the "real world" only through secret channels. The rare individuals who know how to get in touch with a forgery organization are known as fixers, either independent or corporate.

Creating the credit history and the forged stick itself costs money. The greater the detail and reliability of the history required by the client, the higher the rating of the credstick, and the more money it costs to produce.

The Creating A Credstick Table provides information on how much it costs to create a false credstick, if and when a credstick is available, and how long it takes for a client to get a credstick from a top-notch forgery organization. At least half the cost of creating the credstick must be paid to the fixer in advance. For information on using Availability, see either **Shadowtech**, p. 101, or **Shadowrun, Second Edition**, p. 184.

CREATING A CREDSTICK TABLE

Stick Rating	Cost	Availability	Street Index
1–4	Rating x 2,000¥	Rating/12 hours	1
5–8	Rating x 10,000¥	Rating/72 hours	1
9–12	Rating x 50,000¥	Rating/14 days	1
13+	Rating x 250,000¥	Rating/30 days	1

Once created, a credstick is used as if it is the real thing. Under most circumstances, a good forgery will stand up to the verification process and be accepted as legitimate. Only a particularly sophisticated credstick checking and ID verification system might detect a fake.

USING A FORGED CREDSTICK

In order to use a credstick or ID verifier, a player must make an opposed Success Test pitting the rating of the character's credstick/ID against the rating of the verification system. Both sides roll a number of dice equal to their respective ratings, using the opposition's rating as the target number. The side achieving the most successes wins. If both sides achieve the same number of successes, the verifying system instructs the operator to further "interrogate" the credstick bearer. The verifier's display screen will then flash a series of questions based on the bearer's history which the bearer must answer correctly. If the credstick bearer answers any question incorrectly, the verifier rejects the credstick or ID. The character undergoing the further interrogation must make a Negotiation Test (**Shadowrun**, p. 153, or **SRII**, pp. 180–81). The verifier is automatically suspicious of the credstick bearer at this point.

VERIFICATION RATINGS

All credstick checking and ID verifying systems are rated by how efficiently they comb the world's data banks to verify the ID on the credstick. The more efficient the cross-referencing, the higher the rating, and the longer the verification takes.

Rating 1

A Rating 1 verifier provides the most basic credstick check. Able to accept only a passcode for ID verification, average stores or restaurants usually use verifiers of this rating. Other places where illegal credstick use is rare and individual purchases unlikely to exceed 5,000¥ also use this system. The verification process is instantaneous.

Standard Rating 1 units are portable and cost 12,000¥.

Rating 2–3

The Rating 2 or 3 system accepts both passcode and fingerprint identification, and provides instantaneous verification. Rating 2 or 3 systems commonly appear in establishments where most transactions involve less than 20,000¥. Security and law-enforcement vehicles also carry systems of this rating for on-the-spot ID verification. These systems may be portable, but most are linked to the local computer grid either by hardline or cellular connection. Installed Rating 2 or 3 units cost 45,000¥. Portable units cost 60,000¥.

Rating 4–5

Rating 4 or 5 credstick/ID verifiers accept passcode, fingerprint, and voiceprint identification, and the verification process takes 1D6 minutes. These systems usually provide verification service in establishments where most transactions involve less than 200,000¥.

Corporate and private security and law enforcement offices also use Rating 4 or 5 systems to make detailed ID checks. These systems require local computer grid access. They are available only by permit from special sources, and range in price from 100,000¥ to 200,000¥.

Rating 6–7

Extremely sophisticated systems, Rating 6 or 7 ID/credstick verifiers normally check credit history for transactions in excess of 200,000¥. These verifiers also provide ID checks for purposes other than financial. Rating 6 or 7 systems accept passcode, fingerprint, voiceprint, retinal, and cellular print identification, and will verify or reject a credstick within 2D6 minutes.

Elite corporate and private security firms, corporate "information" agencies, and government law enforcement and intelligence agencies favor this rating-level system. A Rating 6 or 7 system also occasionally turns up in the possession of a wealthy or well-connected private individual. These systems require local computer grid access.

Rating 8–9

Rating 8 or 9 systems verify transactions in the 1,000,000¥ range and provide sophisticated ID verification. Used only in the highest reaches of megacorporate and governmental pyramids, these systems are notorious for breaking all but the most solid of forged IDs. They accept all forms of ID verification, and return an okay or denial within 3D6 minutes. Rating 7 or 8 systems require local computer grid access.

Rating 10+

Many people on both sides of the law argue that these legendary systems simply cannot exist. They claim that the enormity of the task of processing the vast amount of crosschecking necessary to conduct so thorough a search makes a system of this rating impractical, if not impossible. No one can provide any details on the capabilities of a Rating 10 system, and only rumor postulates their existence.

Neo Anarchists'
The Guide to
REAL LIFE

Grab the kids! Hide the wife! The Neo-Anarchists are back!

This time, those fun-loving anarchists speak out on everything from transorbital travel and security systems to coffin motels and fast food. Nothing is sacred, profanity reigns, and there's more data than you can shake a chip at.

The NEO-ANARCHISTS' GUIDE TO REAL LIFE provides useful information about the SHADOWRUN world in a fictionalized format along with new, specific game systems for each of the subjects covered. This sourcebook is compatible with the original SHADOWRUN rules as well as the newly revised SHADOWRUN, SECOND EDITION rules.

FASA
CORPORATION