The Decker's Handbook: A Guide to the Matrix

All the rules a Decker needs to run in the SR3 world

Compiled by Keith Rudolph
e-mail: nebular@gamingorgy.com

All of the documentation contained within is taken from the Shadowrun 3rd Edition book. This document is meant to be used as a quick reference for Deckers who may not always have the handbook ready or feel the need to have the Decking section handy at all times. Most of the gamemaster specific information about the Matrix has been removed since the player does not need to know the material.

The Mage's Handbook and The Rigger's Handbook should be released soon to complete the Handbook series.

Compiled by Keith Rudolph
e-mail: nebular@gamingorgy.com

Terminology

Access Control Index Files Slave (ACIFS) – The rating format used when describing the System rating of any host.

Artificial Sensory Induction System Technology (ASIST) – Hardware and programs that allow one to directly experience the senses of another (simsense).

Cyberdeck – A host microcomputer used by deckers for illegal Matrix access; also used by security deckers.

Decker – A hacker, an illegal user of the Matrix.

Direct Neural Interface (DNI) – The ability to interface neural impulses with a computer system, thus allowing a user to interact and control a computer system directly with his brain.

Grid – A series of interlocking computer systems (hosts).

Host – A single computer system.

Icon – Any object a user sees in the Matrix.

Intrusion Countermeasures (IC) – Any software program installed in a computer system (host) with the express purpose of protecting that system from unauthorized users.

Jackpoints – Any physical location that provides access to the Matrix.

Local Telecommunication Grid (LTG) – A Grid covering a small area (neighbourhoods, cities). Numerous LTGs connect to a single RTG.

Matrix – The world telecommunication network.

MPCP – Master Persona Control Program, the master operating system of a cyberdeck.

Node – Part of a host, such as a subsystem, usually represented by a virtual landscape.

Persona – A deckers icon.

Persona Program – One of the four programs (Bod, Evasion, Masking, or Sensors) that defines the personas "Attributes."

Private Locale Telecommunication Grid (PLTG) – Any grid which the general public cannot access.

Regional Telecommunication Grid (RTG) – The largest type of grid, RTGs cover entire countries.

Sculpted System – Matrix hosts with detailed, non-standard iconography, usually encompassing a particular metaphor.

Security Decker – A decker employed by a corporation or law enforcement agency to protect certain Matrix areas from deckers.

Simsense – Hardware and programs that enable a person to experience the reality of what has happened to someone else.

Subsystem – The five operational aspects of any Grid or host, such as Access, Control, and so forth.

System Access Nodes (SANs) – The icon connection between host computers or grids to other host computers or grids.

Tortoise – Decker slang for cyberterminals.

Universal Matrix Standards (UMS) – The standard iconography that is currently falling out of fashion in the Matrix.

Security Levels

Blue – little to no security

- Blue hosts include most public-service databases: newsfax distribution systems, public library databases, directories of listed commcodes – pretty much anything free, whether provided by a government, a corp, or a private individual. Small business too poor to secure their systems tend to have Blue hosts as well.

Green – average security

- Green hosts are average systems, but never make the mistake of thinking that Green host represents easy prey. They may be more patient with intruders than the Orange or Red systems, but they can load any IC the hotter hosts mount.

Orange – significant security

- Orange hosts pride themselves on being secure systems, if not wild-eyed killer hosts. Orange hosts store your standard "confidential" data and carry out process that is important but not absolutely essential to the host's operators. Orange systems include the typical factory controller and the networks used by middle management in a typical corporate office.

Red – high security

- Red hosts offer the most security that a system may legally carry. They contain "top secret" data, often the kind owners will kill to protect, and mission-critical process controls (life support, vital labs and factories, power grids, and the like). Anti-intrusion defenses tend to be lethal – deckers get no "warning shots" on Red systems.

Black – unknown (extreme)

Security Level # is the number of dice the GM uses to oppose a decker's System Tests. Also the number of dice rolled for security tests.

Subsystem Ratings

ACIFS ratings represent the resistance of a system's subsystems to unauthorized manipulation by a decker. These ratings function as a target number for all the test a decker makes when attempting to manipulate they system illegally. For example, an unauthorized decker trying to read files on a system would use his Computer Skill against the Access and Files Ratings of the host in a Success Contest known as a System Test. The Success Contest made against the system's Access Rating would get the decker into the host or grid. The test made against the system's File Rating would enable him to read the files themselves.

Keep in mind that a high subsystem rating does not impede authorized users from using the subsystem. For example, a high Access Rating does not affect the logon procedures of authorized users. It simply makes illegal logon attempts more difficult.

Note that when a Passive Alert has been activated, all Subsystem Ratings are raised by 2.

Access Rating

The Access Rating measures a system's resistance to unauthorized access. To access a grid/host, an unauthorized decker must pit his Computer Skill against the grid/host's Access Rating in a Success Contest.

Control Rating

The Control Rating measures a system's resistance to unauthorized administrative commands. For example, an unauthorized decker attempting to kick a legitimate user off a host must make a Success Contest against the host's Control Rating. Generally, successful tests will enable deckers to reprogram a system or defeat its security measures.

Index Rating

The Index Rating measures a system's resistance to unauthorized searches. An unauthorized decker searching a grid or host for a system address or specific file must make a Success Contest against the grid/host's Index Rating.

Files Rating

Deckers must make a Success Contest against the Files Rating whenever they attempt to illegally read or write datafiles in a system. Deckers must also make tests to decrypt encoded files and send output to devices such as faxprinters or chip cookers.

Slave Rating

The Slave Rating governs the operation of remote devices controlled by a system. For example, a Success Contest against the Slave Rating enables the unauthorized decker to take control of devices manipulated by a host, such as security cameras and elevators.

Rating Format

System Ratings use the following shorthand format:

Security Code-Security Value/Access/Control/Index/Files/Slave

For example, a Red-6 system with Access and Index Ratings of 10, a Control Rating of 12, and Files and Slave Ratings equal to 9 would be written:

Red-6/10/12/10/9/9

The acronym "ACIFS" – Access Control Index Files Slave – is frequently used

CYBERDECKS

Deck Ratings

The power of a decker's persona is defined by the processing power of his deck's MPCP (Master Persona Control Program), and his Bod, Sensor, Evasion, and Masking programs. The MPCP represents the master operating system for the deck and has an MPCP Rating that measures its ability to take damage and continue functioning. The Bod, Sensor, Evasion, and Masking programs are called persona programs. The numeric ratings of these programs serve as the "Attributes" for the decker's persona and are used whenever tests are made against the decker while in the Matrix. Deckers also use utility programs, rated in the same manner.

The MPCP Rating is the central value of cyberdecks. The MPCP Rating multiplied by 3 equals the maximum total of the deck's persona programs. No single Persona rating may exceed the MPCP Rating, and the maximum value for utility programs is equal to the MPCP Rating.

The shorthand format for describing a cyberdeck's ratings is:

MPCP Rating/Bod Rating/Evasion Rating/Masking Rating/Sensor Rating

A deck with MPCP-9 and all Persona programs distributed equally among the maximum total (3 x 8 = 24), would be written as MPCP-8/6/6/6/6.

Hardening

Hardening represents internal deck programs specifically designed to reinforce the deck's resistance to invasive code such as viruses, gray and black IC, etc.

For every point of Hardening, reduce the Power of any Damage from Black IC to the on-line icon or the actual decker by 1 for Resistance tests. If your icon has been crashed by gray IC and it makes an Attack Test, for every 1 point of Hardening, add 1 to the Target Number for the Attack Test.

Hardening also works against the Black Hammer and Killjoy utilities, but not against other attack utilities.

Active Memory

Active memory is the cyberdeck's "RAM," to use the old-tech term.

A deck's active memory limits the utility programs the deck can run at any one time. For each Mp of Active Memory the deck can have the equivalent Mp in utilities. For example, a deck with 200 Mp of active memory can run no more than 200 Mp of utilities at any one time.

Storage Memory

Any program in a deck's storage memory can be loaded onto the deck by using the Swap Memory operation.

All utilities must be kept in storage memory, regardless of whether you have them in active memory or not. Additionally, storage memory is used for data uploads and downloads. The total amount of MPs for all utilities, and other stored data cannot exceed the storage memory of the deck.

I/O Speed

All uploads and downloads are always at the full I/O speed of the deck, in Mp per Combat Turn.

Response Increase

Response Increase is the Matrix equivalent of wired reflexes. Each point of Response Increase increases a persona's Reaction Attribute by 2 and Initiative by +1D6.

A deck can support only 3 points of Response Increase. Furthermore, Response Increase cannot exceed a deck's MPCP Rating divided by 4, rounding fractions down (so a deck with MPCP Rating 3 or below cannot sustain any level of Response Increase).

Detection Factor

The gamemaster uses the decker's Detection Factor as the target number when making test to detect a decker's presence or prevent a decker from performing actions within the Matrix. To determine the decker's Detection Factor, calculate the average (round up) of the decker's Masking Rating and Sleaze program rating. For example, an MPCP-8/6/8/6/4 deck, running a Sleaze-8 program, would have a Detection Factor of 7. That [6 (Masking) + 9 (Sleaze) = 14] divided by 2 = 7.

If a decker is not running a Sleaze program, the Detection Factor equals half of the Masking Rating.

The Hacking Pool

The Hacking Pool follows all the normal rules of dice pools. To determine a decker's Hacking Pool, add the decker's Intelligence Rating and her deck's MPCP Rating, divide the total by 3 and round down. (Any increases to a decker's Intelligence apply to her Hacking Pool as well, whether they come from cyberware or magic. Increases are cumulative.)

Generally, Hacking Pool dice may be added to any test made in the Matrix.

Hacking Pool dice cannot be used in Body or Willpower Tests made to resists the effects of gray or black IC that is damaging the decker. Only Karma Pool dice, enhancements connected to the cyberdeck, or magic boosts to the decker's Body or Willpower can help in such situations.

Accessories

Cyberdecks and cyberterminals frequently come with accessories such as off-line storage, or a vid-screen display so that others may should-surf the Matrix going-ons from the decker's point-of-view. Hitcher jacks, whether electrodes or datajack feeds, allow others to "jack in" and shoulder-surf directly, as

the decker's icon. Hitcher cannot manipulate or effect the decker's persona in any way, they are merely along for the ride. Hitchers are also protected from nasty IC side-effects.

RUNNING THE MATRIX

Movement in the Matrix

Movement in the Matrix is virtually instantaneous unless the decker is engaged in Matrix combat, attempting to deal with IC, performing system operations, transferring data, or loading programs. In the Matrix, data is transmitted at megabaud rates, and system response is measured in microseconds. Only when dealing with something that requires real attention does the action slow down there the decker can notice time passing.

When moving in the Matrix, distance is entirely relative.

Subjective Time

Keep in mind that characters experience time somewhat subjectively in the Matrix. The apparent time spent moving through the Matrix environment may be much longer than the actual game time used to perform actions. For example, a decker who makes a single system operation to find a file may experience the test as a walk down a long hallway lined with books, which ends when he finds the icon he wants. He may feel as if he has spent several minutes or even hours searching, when actually only a few seconds of game time have elapsed.

Exiting the Matrix

A decker can leave the Matrix any time by jacking out, pulling the plug that connects his datajack to the deck. Keep in mind that the decker's Matrix-image, the persona, is only a program running on the computers of the Matrix. Jacking out is a Free Action unless the decker is under attack by Black IC.

A decker kicked out of the Matrix involuntarily has been dumped. The rapid cutoff of the deck's simsense signal can cause the decker to experience mild disorientation known as Dump Shock.

Matrix Perception

Noticing New Icons

Whenever a new icon, such as a decker or program, enters the area currently occupied by the decker, she may make a free Sensor Test (no utilities allowed), to see if she becomes aware of the new icon. The target number for this test is Masking Rating + sleaze utility if the icon is a decker, or the icon's rating if it is IC or another program. Only 1 success is necessary to detect the icon (if the icon is IC, 2 successes will tell you the type and 3 will reveal the rating), although the decker may not know what the icon represents unless she performs an Analyze Icon operation. Once located, the icon remains "visible" unless is maneuvers to escape the decker. This Free Action represents the capability of the deck's sensors in identifying other programs. If the Sensor Test fails to detect the icon, the decker is unaware of its presence until it chooses to reveals itself or attacks her.

If a decker suspects the presence of another icon, she can use a Locate operation to verify the suspicion.

Noticing Triggered IC

Deckers don't always know when they have triggered IC. Before a decker can attack IC or take other measures to neutralize it, a decker must first "locate" the IC.

Reactive IC Is more insidious, because it does not betray its presence to the decker by any actions. Whenever a decker triggers reactive IC, the gamemaster secretly makes a Sensor Test against a target number equal to the IC's Rating. If the test results in 1 success, the gamemaster informs the decker that her actions triggered IC. On 2 successes, the gamemaster tells the decker the type of IC triggered. On 3 or more successes, the gamemaster reveals the IC's Rating and location. This Sensor Test is made only once, when the IC becomes active.

If a decker suspects the presence of active IC, she can use the Locate IC operation to check out that suspicion.

Non-Combat Actions

For non-combat actions, deckers need not roll for initiative. Instead, divide the decker's Reaction Attribute (augmented by Response Increase) by 10 (round up the result). The result is the number of actions the decker may perform during each 3-secon game turn. Add 1 action for every Initiative die the decker receives in the Matrix beyond the standard 1D6.

For example, a decker with 2 actions per turn could perform a Logon to Host operation (a Complex Action) and an Analyze Icon operation (a Free Action) on his first Initiative Pass. On the next action, he could perform an Analyze Host operation (a Complex Action).

Reactive IC programs that perform tasks at the end of a Combat Turn act after all deckers have performed their allotted actions for a turn.

SYSTEM TEST

In order to perform specific tasks in the Matrix, a decker submits a command or series of commands to the host/grid. These commands are known as system operations. Each such operation requires a specific game action (Free, Simple, or Complex) and is affiliated with a specific subsystem (Access, Control, Index, Files, and Slave), all noted under their individual descriptions.

In addition, unauthorized deckers must make a test – known as a System Test – whenever they attempt to perform system operations within the Matrix. This is due to the fact that as unauthorized Matrix users they must coerce various computer systems to commit processing time and power to their tasks. The more a decker tasks a system, the more likely the system is not become aware of the intruder and activate countermeasures.

System Teas are always resolved as a Success Contest between the decker and the target host/grid. The decker uses his Computer Skill (or specialization in Decking) to make a test using the Systems Rating appropriate to the operation his is attempting as the target number. The target number for theses tests may be modified by appropriate utility programs the decker is running. Hacking Pool may be used for System Tests.

At the same time, the host/grid rolls makes a Security Test, rolling its Security Value against a target number equal to the decker's Detection Factor.

If the decker achieves more or an equal amount of successes than the host/grid, he wins the Success Contest and succeeds at whatever task he is attempting to perform. If the host achieves more successes, the decker fails.

Regardless of the test outcome, the gamemaster records the host's number of successes and adds the total to any previous successes the host achieved in System Tests against the decker. This running total creates the security tally.

System Operations on Grids

Certain locations, such as the physical jackpoint at the beginning of a run, can limit a decker's options in terms of system operations. In addition to the following system operations, deckers can always perform a Graceful Logoff operation at any time.

From a Jackpoint

Deckers jacking in vial legal or illegal telecom connections can only perform the Logon to LTG operation. Then they have to find the host/grid they want to invade, if they don't know its location. Deckers jacking in via a dedicated workstation, slave-controlled remote device, or console can only perform the Logon to Host operation and must log on to the host that controls the gizmo they are using for access.

On an LTG

Once logged on to an LTG, the decker can move to the parent RTG with a Logon to RTG operation or try to access any host connected to the LTG with a Logon to Host operation. If a PLTG is attached to the LTG the decker is on, he can use a Logon to LTG to try and break into it.

On an RTG

Once logged on to an RTG, the decker can either move to another RTG by using a Logon to RTG operation or enter any LTG attached to the RTG with a Logon to LTG operation.

The character may also perform the Located Access Node operation on an RTG.

On a PLTG

A decker logged on to a PLTG may perform nay System Operation available on public RTGs and LTGs.

SECURITY TALLY

The gamemaster tallies all the successes a host/grid achieves while opposing a decker in System Test,. This includes all success made, not just net successes. This tally runs as long as the decker is logged on to that particular host/grid. When the tally reaches a level set by the gamemaster, it may trigger actions within the host/grid, ranging from the activation of black IC program to nothing at all. The bottom line is that a decker never knows what will happen as a result of his next test, or how many more tests he can safely afford before the host/grid catches on to his presence and does its best to crash him.

Security Sheaves

A security sheaf describes the security measures in place on a host or grid as well as how the host/grid reacts to intruders. Quite simply, a sheaf consists of a list of trigger steps. These steps represent security tally thresholds. As a decker's security tally reaches each trigger step, the system activates one or more IC programs. Trigger steps also activate he various alert levels in a system. The alert status of the system, in turn, affects the type of IC programs they system activated.

The security code of the host/grid determines the frequency of rigger steps in a system, and the gamemaster determines the events activated by each trigger step.

Trigger Steps

As noted above, trigger steps consist of specific security tally number. Whenever the security tally of a decker reach or exceeds one of a system's trigger steps, the system automatically activates one or more security measures, such as IC programs or alerts. Low-security systems, such as Blue hosts, maintain few trigger steps – as a result, they have fewer IC programs and other security measures. High-security systems, such as Red hosts, set trigger steps in small increments, and so they have more IC programs and security measures.

Multiple Triggers

If a decker performs several actions on a system that together add a large number of points to his security tally all at once, the increase may cover two or more trigger steps. In this case, the indicated events for ALL the triggered steps that have been reached or exceeded occur at once.

Grid Security Tallies

Switching LTGs within the same RTG does not affect the security tally against a decker. The tally does not follow the decker if he logs on to another RTG.

PLTGs and Security Tallies

Because PLTGs maintain very active security routines, a security tally built up under a give RTG does remain in force if the decker logs on to a PLTG from the RTG. This occurs because PLTGs pick up security "flags" from RTGs when they acknowledge logons. This means that a decker who racks up a big tally working his way through the public grids may trigger IC as soon as he enters private dataspace.

Alerts

All systems have three alert statuses – no alert, passive alert, and active alert. The normal status for all systems is no alert, and active alert. The normal status for all system sis no alert. Specific trigger steps activate passive and active alerts. In turn, the alert status of a system determines the types of IC programs that go into action at the system's trigger steps.

No Alert

Generally, trigger steps under a no alert status activate reactive IC programs.

Passive Alert

Passive alert means that a system suspects an intruder has invaded it, but is not 100% certain. Under passive alert status, trigger steps typically activate proactive white or gray IC programs.

When a system goes on passive alert status, increase all Subsystem Ratings by 2.

Active Alert

Active alert means the system has verified the presence of an illegal icon.

Under active alert status, trigger steps typically activate proactive and sometimes black IC programs. Trigger steps may also activate corporate law-enforcement deckers in the system.

Once a system reaches active alert status, running away and sneaking back into the system becomes much more difficult for illegal deckers. Security personnel know that someone has been snooping around, and the system managers remain particularly vigilant for some time to come.

Host/Grid Reset

Blue systems reset completely in 2D6 minutes, during which the system deactivates security measures and the security tally drops to 0. More secure system do not reset as quickly. Green, Orange, and Red systems being to reset after 3D6 minutes, provided the decker did not trigger a passive or active alert.

If a decker triggers an alert on a Green, Orange, or Red host/grid, the system resets even more slowly. Roll 1D6 every 5 minutes for Green systems, every 10 minutes for Orange system, and every 15 minutes for Red systems. Reduce the system's security tally by the result.

TRIGGERING IC

IC (pronounced "ice") standard for intrusion countermeasures. Some IC just impedes the decker, maybe tries to get a network ID on him. Other programs are designed to crash his icon off the Matrix. Still other go after his deck. Finally, there's black IC – which flat out tries to kill him.

Proactive vs. Reactive

IC is either proactive or reactive. Proactive IC attacks the decker in cybercombat once it is alerted to his presence. Proactive IC attacks like a hostile NPC. It makes Initiative rolls during combat, maneuvers for advantage, and uses its weapons and other tricks.

Reactive IC, on the other hand, just "sits there." It may activate when the security tally reaches a specific threshold, decker actions may trigger it, or it may reside in a specific location or resource of the host, such as a file, slave remote, or even an entire subsystem. In the latter case, the IC becomes active when a decker accesses the protected location or resource. Once a decker triggers reactive IC, the IC affects the decker's operations until the decker destroys or deceives it, or otherwise convinces it to go away.

Crashing IC

Whenever a decker "kills" or crashes IC in cybercombat, add the rating of the crashed IC to the decker's security tally. The rationale for this is that crashing IC is like opening up on a perimeter guard with full autocannon fire – the action destroys the guard but alerts his colleagues that company's coming.

Suppressing IC

A decker can avoid the penalty for crashing IC by suppressing it when he destroys it. However, suppressing IC lowers a decker's Detection Factor. Reduce a decker's Detection Factor by 1 for each IC program he suppresses. This reduction remains in effect as long as the decker remains in the system, unless he releases the suppressed IC.

Deckers must declare their intention to suppress IC as soon as they crash it. Decker's may "unsuppress" or release IC at any time. For each IC program the decker releases, he regains 1 point to his Detection Factor. His security tally, however, increases by the appropriate amount for each released IC program.

Deckers cannot suppress IC in a system they have left.

IC Ratings

Each IC program has its own rating. The rating measures the damage the IC does or acts as a target number for tests the decker makes to avoid its effects.

Types of IC

There are three specific types of IC.

White

White IC is only programmed to attack a decker's on-line icon and cannot permanently damage the decker or his deck.

Gray

Gray IC is designed to specifically target the decker's cyberdeck and utilities, which can result in permanent damage.

Black

Black IC is specifically programmed to attack the decker himself, creating dangerous biofeedback between the decker and his cyberdeck, possibly leading to permanent physical and psychological damage or even death.

SYSTEM OPERATIONS

Every system operation consists of three parts: a System Test, an appropriate utility, and a type of game action.

The System Test indicated which type of Success Contest the decker makes to perform the action: Access Test, Control Test, Index Test, Files Test, or Slave Test. Each test uses the appropriate Subsystem Rating of the host/grid as the target number. Each operation description lists appropriate utilities that deckers may use to reduce the target number for the System Test. As part of the Success Contest, the gamemaster makes an opposed Security Test for the host/grid against the decker's Detection Factor.

The action listed in each operation entry describes what type of game action – Free Action, Simple Action, or Complex Action – the decker must spend to perform the operation.

Most system operations fall into one of three broad categories: interrogations, ongoing operations, and monitored operations.

Interrogations

In most system operations, a decker give the host/grid system an order, which the system immediately carries out. During interrogation operations, however, a decker engages in a "dialogue" with a system as he searches for specific information. A decker may have to repeat an interrogation operation more than once to locate the exact file or slave control that he needs.

The following operations are interrogation operations: Locate Access Node, Locate File, Locate Slave.

Ongoing Operations

Some operations are finished as soon as the decker succeeds at the System Test. Other operations, such as uploads and downloads, take time. In these ongoing operations, the decker beings the operation, then allows it to run without giving it any further directions.

The time required for ongoing operations is measured in seconds, according to the rules for the specific operation.

The following are ongoing operations: Download Data, Swap Memory, Upload Data.

Monitored Operations

Monitored operations must be carefully controlled after they are set in motion. After a decker makes the initial System Test to begin a monitored operation, he must sped a Free Action to maintain the operation each Initiative Pass. If he fails even once to sped these actions, the operation aborts and he must repeat the operation System Test to restart it.

In some cases, allowing a monitored operation to abort may result in irreversible consequences in the real world. For example, a decker may be running an Edit Slave operation that prevents a security camera from showing human guards the image of the decker's companions breaking into their facility. If the decker allows the Edit Slave operation to abort, the guards may see the decker's companions and foil the run – or worse.

The following are considered monitored operations: Control Slave, Edit Slave, Make Comcall, Monitor Salve, Tap Comcall.

All operations are in Appendix A

UTILITIES

Utilities come in four varieties: operational, special, offensive, and defensive. Operational utilities apply to a decker's System Tests. These provide especially useful when performing system operation, hence the name operational utilities. Special utilities perform specific tasks in the Matrix. Offensive utilities are used to damage opposing deckers, IC programs, and so on. Defensive utilities are designed to prevent or reduce the damage taken in cybercombat.

The multiplier value listed in each utility entry is used to determine program size. Each listing also notes any system operations for which the utility may be used.

Utility programs come in two formats, the original source code and copies. A decker must have the source code of a program to upgrade or modify the program.

Unless otherwise noted, utility programs must be pre-loaded into active memory to work.

All utilities are in Appendix B

CYBERCOMBAT

Decker Initiative

The Initiative of a decker is based on the Reaction Attribute of the decker's persona. If his Reaction has no enhancements, the decker roll 1D6 and adds the result to his Reaction to determine Initiative.

Each level of Response Increase adds 2 to a decker's Reaction and +1D6 to his Initiative.

Wired reflexes, magical augmentations, vehicle-control rights, and other enhancements that increase the Reaction Attribute of a decker's physical body do not affect Initiative in the Matrix.

Initiative and the Physical World: If a decker is engaged in direct communication with the physical world via video, print, datascreen, and so on, he loses 1D6 of Initiative until he drops the communications link. This penalty does not apply to communications with a meathead via hitcher electrodes, nor does it apply to users with tortoises.

Actions

Any icon may take one Free Action, and either two Simple Actions or one Complex Action during a Combat Phase.

Besides the actions listed here, deckers may perform system operations. Deckers must perform specific actions to execute each operation.

Free Actions

Free Actions are simple, almost automatic actions that require hardly any effort to complete.

The following system operations are Free Actions: Analyze IC, Analyze Icon.

Delay Action: Deckers may delay actions per standard rules.

Jack Out: A decker can jack out of the Matrix anytime as a Free Action, unless she has been attacked and successfully hit by Black IC. If the decker has not performed a Graceful Logoff operation before jacking out, she is susceptible to Dump Shock.

Speak a Word: Standard rules apply for verbal communications. Direct communications with characters in the physical world affect the decker's Initiative as noted in the above Initiative section.

Deckers may also "buffer" messages. When buffering a message, the decker may write a message up to 100 words long and give it to any character lined to the decker with hitcher electrodes, radiolink, datascreen, or other device. The second character may also operate an icon the decker can "see." The second character receives the buffer message at the end of the Combat Turn.

Terminate Download/Upload: A decker can suspend or terminate a data transmission at any time.

Unload Program: The decker can remove a program from his deck's active memory at any time. Removing a programming releases active memory for a Swap Memory operations.

Unsupress IC: A decker can release IC from suppression and restore the points being used to suppress the IC to his Detection Factor at any time. If the suppression was keeping crashed IC from increasing the decker's security tally, the tally increases immediately. If the suppression was suspending the IC's actions, it becomes active immediately.

Simple Actions

A Simple Action requires a bit more concentration to perform than a Free Action, and may be slightly more complex.

The following system operations are Simple Actions: Analyze Security, Analyze Subsystem, Decrypt Access, Decrypt File, Decrypt Slave, Download Data, Edit File, Monitor Slave, Swap Memory, Upload Data.

Attack: A decker may attack an icon with any offensive utility loaded in his deck. IC programs and other icons may attack according to their programming.

Combat Maneuvers: Deckers and icons may engage in any listed combat maneuvers as a Simple Action.

Complex Actions

Performing a Complex Action requires intense concentration on only that task. Certain System Operations require a complex action, as well as attempting to jack out after having been attacked by Black IC.

The following system operations are Complex Actions: Analyze Host, Control Slave, Edit Slave, Graceful Logoff, Locate Access Node, Locate Decker, Locate File, Locate IC, Locate Slave, Logon to Host, Logon to LTG, Logon to RTG, Make Comcall, Null Operation, Tap Comcall.

Combat Maneuvers

Deckers, proactive IC, and any other self-directed icons can perform combat maneuvers to avoid detection, parry attacks, or gain a position to make more accurate attacks. All combat maneuvers are Simple Actions.

Each combat maneuver requires an Opposed Test between the icon performing the maneuver and the icon opposing the maneuver. The maneuvering icon pits its Evasion against the opposing icons Sensor Rating. If either icon is an IC program, substitute Security Value for the Attribute.

If the maneuvering icon achieves more successes, note the net successes – the number of successes that exceed the opposing test successes. The net successes determine how successfully the icon maneuvered. If the opposing icon achieved an equal or greater number of successes, the combat maneuver fails.

If the maneuvering icon has a cloak utility, reduce the icon's target number by the Utility Rating. If the opposing icon has a lock-on utility, reduce its target number by the Utility Rating.

Hacking Pool can be added to these tests.

Evade Detection

An icon may perform and evade-detection maneuver to evade an opposing icon that has detected it.

A decker must use the Locate IC operation to re-detect an IC program that has evaded him with the maneuver. To re-detect personas that have evaded him, a decker must use a Locate Decker operation.

Parry Attack

The parry-attack maneuver enables the maneuvering icon to enhance its defenses in cybercombat. If the maneuvering icon wins the Success Contest, increase target number for attacks against the icon by its net success on the test.

The bonus lasts until the next attack by the opposing icon. If the opposing icon performs a position attack maneuver, the maneuvering icon retains the parry bonuses. If either icon successfully performs an evade detection maneuver, the bonus is lost.

Position Attack

The position attack maneuver enables an icon to position itself for an attack on an opponent. This is a dangerous maneuver that may backfire on an icon. If the maneuvering icon wins the Success Contest,

the icon may reduce the target number for its next attack by its net successes or increase the Power of its attack by the net successes. If the opposing icon wins the Success Contest, that icon receives the bonus.

The bonus lasts only until the next attack.

Resolving Attacks

To make an attack, the attacker makes a test with his offensive utility program. (Hacking Pool dice may be used to augment the program.) The target number for the test depends on two factors: the target icon's status – Legitimate or Intruding – and the Security Code of the host where the attack occurs. Any decker icon or IC program that has logged onto a system with a valid passcode is considered Legitimate. All other icons are Intruding.

If a decker has somehow acquired a Legitimate passcode, or previously planted one on the host, he may log in using it. In general, if the decker uses that passcode to take advantage of Legitimate status during a fight with the host's own security programs, the host devalidates the passcode when the decker jacks out or logs off. He has blown his cover, so to speak. However, he can use the passcode in combat against Intruding deckers without blowing his cover.

Record the number of successes scored on the Attack Test, because they determine the effects of the attack. The various types of offensive utilities have different effects on their targets, but most inflict damage on a decker's physical body. Any special effects and test made by e the targeted icon are noted in the offensive utility description.

Icon Damage

Many programs, such as attack and killer IC programs, inflict damage per standard rules. Each of these program has a Damage Code, which consists of a numeric Power and Damage Level.

The Damage Level for such IC programs is determined by the host's Security Code.

The icons that has been hit rolls a Damage Resistance test using its Bod Rating against a target number equal to the Power of the damage. For IC program that take damage, make a Damage Resistance test using the host's Security Value. The armor utility reduces the Power for the test.

Condition Monitors

All icons use the standard Condition Monitor, although they use only one damage track – there is no Stun damage to icons. Damaged icons suffer target number modifiers as indicated on the Condition Monitor. If all 10 bones on an icon's Condition Monitor are filled, the icon crashes. If the icon is a persona, the persona's decker is dumped from the Matrix. The decker is vulnerable to Dump Shock and possibly other effects.

Simsense Overload

Whenever a decker's icon takes damage from white or gray IC, the decker's physical body may suffer Stun damage through a resonance effect over the ASIST interface.

To determine whether the decker takes simsense overload damage, he makes a Willpower Test against a target number based on the damage take by his icon. These target numbers are provided in the Overload Damage Target Numbers table. Any icon that takes Deadly damage crashes automatically and exposes the decker to Dump Shock.

If the Willpower Test fails, the decker suffers a Light Stun wound and fills in 1 box on his Mental Condition Monitor.

Dump Shock

When a decker is crashed off the Matrix or jacks out without performing a Graceful Logoff operation, he risks Stun damage from Dump Shock. The Power of the damage equals the host's Security Value. This measures the shock of the sudden transition from virtual to physical reality. The Damage Level is determined by the host's Security Code, as shown on the Dump Shock Damage Levels table.

INTRUSION COUNTERMEASURES

White IC

White IC affects only the decker's on-line icon. It attacks the icon's ratings but does not affect the cyberdeck's permanent ratings or utilities. The worst white IC can do is dump a decker or scramble data she is trying to read or write.

Cripplers

Cripplers are proactive white IC programs that each attack one of the decker's icon's Attributes. Cripplers come in four types: acid, binder, jammer, or marker programs. Acid cripplers attack an icon's Bod Rating, Binder cripplers attack an icon's Evasion Rating, Jammer cripplers attack the Sensor Rating, and Marker cripplers attack the Masking Rating.

Whenever a crippler program attacks an icon, they engage in a Success Contest. The gamemaster makes an Attack Test for the host and tallies the successes. At the same time, the decker makes a test using the affected icon Attribute against a target number equal to the crippler IC's Rating. If the decker achieves a greater or equal number of successes, the IC does no damage. Reduce the affected icon attribute by 1 point for every 2 net successes the IC scores.

Neither Armor nor Hardening protect against cripplers.

Crippler IC cannot reduce an icon Attribute below 1.

Killer

Killer IC is proactive IC that causes damage to icons in cybercombat. All killer IC has a Damage Code and its Power is equal to its IC Rating. The Damage Level of killer IC is based on the host's security code. Killer IC on Blue or Green systems does Medium damage; killer IC on Orange and Red system does Serious damage.

Armor programs reduce damage from killer IC.

Probe

Probe IC is reactive IC that conducts additional interrogations of data packets and program requests for computer resources. Probe IC helps detect any operations performed by unauthorized programs.

For a probe-equipped system, the gamemaster makes a Probe Test using its probe IC Rating against the decker's Detection Factor every time the decker makes a System Test. Add any success from the Probe Test to the decker's security tally.

Scramble

Scramble IC is reactive IC used to protect elements of a host's Access, Files, or Slave subsystems. Scramble IC can be programmed to protect a specific component of a subsystem or the entire subsystem.

Scramble IC programs are designed to make it impossible to Access any host or slave devices they protect, unless it is decrypted. Additionally, scramble IC will destroy the data under its care rather than letting it fall into unauthorized hands. If the decker tries to decrypt scramble IC and fails, the gamemaster makes a Scramble test using its Rating against a target number equal to the decker's Computer Skill. If the test fails, the decker has managed to suppress the scramble IC's destruct code. If the test succeeds, the data is destroyed.

Deckers may use specific system operations to defeat scramble IC, all of which can be augmented by the decryption utility program. Decrypting scramble IC does not add to the decker's security tally. Deckers can use attack program to crash scramble IC, but doing so will increase the decker's security tally unless he suppresses the scramble IC.

Tar Baby

Tar baby is reactive IC that attempts to crash deckers' utility programs. Each tar baby is pre-programmed to target a specific type of utility (operational, offensive, defensive, special), determined by the gamemaster. Tar baby IC does not attack completely passive utilities such as armor and sleaze programs.

Whenever a decker uses one of the trigger utilities, the gamemaster make an Opposed Test between the two programs' ratings. Make the Tar Baby Test against a target number equal to the utility program's rating. Make the Utility test against a target number equal to the tar baby IC's Rating.

If the tar baby wins the Opposed Test, it crashes both itself and the utility program. Tar baby IC does not increase the decker's security tally when it crashes this way. The decker also has to load a fresh copy of the utility program with a Swap Memory operation.

If the utility wins the Opposed Test, it remains safe and the gamemaster makes a secret Sensor Test to determine if the decker notices the tar baby IC.

Gray IC

Gray IC programs attack a decker's cyberdeck and utilities directly. Any damage caused by gray ID attack permanently affects the deck's ratings. Damaged chips and other components must be replaced to restore the deck's original ratings.

Blaster

Blaster IC is proactive IC that attacks in cybercombat in the same manner is killer IC. Armor reduces the damage from blaster attacks.

Additionally, blaster IC may permanently damage a decker's MPCP if it crashes his icon. If blaster IC dumps a decker, make a Blaster Test using its Rating against a target number equal to the deck's MPCP Rating. Hardening increases the target number but armor has no effect. Reduce the MPCP Rating by 1 point for every 2 successes on the Blaster Test. Note that the decker may need to crank down his persona programs if his deck takes damage, because their total may not exceed the deck's MPCP Rating multiplied by 3.

Rippers

Ripper IC is a gray version of crippler IC. This proactive IC attacks in the same manner. In addition, whenever a ripper program reduces an icon Attribute to zero, make a Ripper Test using its rating against a target number equal to the deck's MPCP Rating (Hardening increases the target number). For every 2 successes on this test, reduce the MPCP Rating by 1. Replacing the persona chip is the only way to restore this damage.

Four different types of riper IC exist: acid-rip, bind-rip, jam-rip, and mark-rip. Acid-rip, also known as "bod-stripper", "sizzler", or "peeler", attacks the deck's Bod Rating. Bind-rip, also known as "gluefoot", "mummy" or "flypaper", attacks the Evasion Rating. Jam-rip, also known as "blinder", "gouger", or "stick", attacks the Sensor Rating. Mark-rip, also called "screamer", "pain", or "tag", attacks the Masking Rating.

Sparky

The proactive IC called sparky IC attacks in the same manner as killer IC. However, if sparky IC crashes the persona, it causes an overload in the deck's power supply that feeds random jolts of electricity to the MPCP and the decker's brain. Results can range from a little impromptu electroshock therapy to a killing jolt.

Whenever sparky IC crashes a persona, make Sparky Test against a target number equal to the deck's MPCP Rating + 2. Hardening increases the target number. Reduce the MPCP Rating by 1 point for every 2 successes of the Sparky Test. A sparky attack also causes (IC Rating)M damage to the decker. Stage the Damage up one level for every 2 successes on the Sparky Test. The decker resists this damage as he would any other. Hardening reduces the Power of the damage.

Tar Pit

The reactive IC known as tar pit IC operates and attacks in the same manner as tar baby IC. However, if tar pit IC trashes a utility on-line, it also injects the deck with viral code that corrupts all copies of the program in the deck's active and storage memory. Unless the decker has a backup copy of the utility stashed in off-line memory, he's lost it for good. And even if he has a backup, he can't get at it for the rest of the run.

When tar pit IC trashes a program, make a Tar Pit Test against a target number equal to the deck's MPCP Rating. Hardening increases the target number. If the test produces no successes, the viral code is defeated and the tar pit IC has the same effect as the tar baby program, so the decker can reload his utility with a Swap Memory operation. If the Tar Pit test produces any successes, however, the IC corrupts all copies of the program stored on the deck. The decker cannot get the utility back until he jacks out and reloads the utility from a source outside his deck.

Black IC

Black IC is a form of proactive IC that sample the command transaction between the decker and his deck and then injects dangerous biofeedback responses into the deck's ASIST interface. These feedback responses raise the deck's simsense signal to the same levels as a BTL chip on overdose intensity. As a result, the signal may overload the decker's neural connections and in turn render him unconscious, trigger psychological disorders, brainwash him, or cause death from a stroke, heart failure, respiratory paralysis, aneurysm, or neurotransmitter autotoxicity. And those are just a few of the possible effects.

Black IC in Combat

Black IC begins to subvert the ASIST interface in a decker's cyberdeck as soon as it scores a successful attack on the decker, even if the hit does no damage. Until the IC scores that first attack, jacking out of the Matrix is a Free Action.

After a black IC hit, the decker must spend a Complex Action and make a successful Willpower (Black IC Rating) Test to jack out. If the test succeeds, the decker may jack out, but the black IC Makes one more cybercombat attack against him before the connection goes down. Black IC also makes an automatic attack if a companion at the jackpoint pulls the plug when the deck indicates black IC activity.

Lethal Black IC

Lethal Black IC fights like killer IC in cybercombat. However, successful lethal black IC attacks cause damage to a decker and his icon. The Damage Code for the IC depends on the Security Code of the Host: (IC Rating) Moderate for Blue and Green Systems, (IC Rating) Serious for Orange and Red ones. The Damage Code applies to damage to both the decker and his icon.

Stage up the Damage Level for every 2 successes on the IC's Attack Test. Every time black IC hits a decker, the decker rolls two Resistance Tests. Hardening reduces the Power of the damage for these Resistance Tests. A Body Resistance Test, using his Body Attribute, enables the decker to resist damage to his person. The Hacking Pool may not be used for this test, though Karma Pool dice may be. The decker also makes a Resistance Test using his icon's Bod Rating to resists damage to the icon. The icon resists damage as it resists damage from killer IC, and armor protects the icon normally.

The decker's Matrix connection remains intact if the icon is killed before the decker dies or manages to jack out. In such cases, the IC completely dominates the decker's icon bandwidth. Increase the effective rating of the IC by 2. Of course, the decker cannot fight back at all with his icon down. All he can do is try to jack out before the IC kills him.

The Matrix connection automatically goes down if the black IC kills the decker. But before it turns the deck loose, the black IC gets a shot at the MPCP, making the attack as if it were blaster IC, with double its rating. If the black IC completely destroys the MPCP, the IC deletes all data downloaded by the decker during the run. It deletes any such data stored in any connected storage memory as well, and reduces the MPCP's Rating to 0.

Permanent Effects: Lethal black IC damage overflows in the same manner as Physical damage to a character. Any Deadly wound may produce permanent after-effects. Overflow damage from lethal black IC. Represents increased levels of brain damage. In addition to permanent damage, these after-effects may include neurological damage that produces memory lapses, hallucinations, tremors, phantom pain, migraines, or similar conditions. In the case of neurological damage, the gamemaster may devise his own rules for the long-term effects. However, if the decker can be revived, all the rules for Deadly damage apply.

Non-Lethal Black IC

Non-lethal black IC function in the same manner as lethal black IC, with the following exceptions. First, non-lethal black IC causes Mental, not Physical damage. Deckers resist such damage with Willpower test. If damage from non-lethal black IC renders a decker unconscious, the decker's Matrix connection is automatically broken. However, the non-lethal black IC still gets a final shot at the cyberdeck's MPCP and the data downloaded during the run.

Mental damage done by non-lethal black IC can overflow into the Physical Condition Monitor.

Appendix A
System Operations

Analyze Host

Test: Control
Utility: Analyze
Action: Complex

Any Analyze Host operation enables a decker to analyze the ratings of a host. For each net success in the System Test, the decker chooses one of the following pieces of information which the gamemaster supplies:

- The host's Security Rating (code and value)
- The rating of any one of the five subsystems on the host

Seven or more successes gain the decker all the available information about the host. Note that a decker must be on the host to run an Analyze Host operation on it.

Analyze IC

Test: Control
Utility: Analyze
Action: Free

The Analyze IC operation enables a decker to identify any specific IC program that he has located. If the Analyze IC operation succeeds, the decker learns the type and rating of IC program and any operations or defenses it carries.

Analyze Icon

Test: Control
Utility: Analyze
Action: Free

The Analyze Icon operation scans any icon and identifies its general type: IC, persona, application and so on. The decker may reduce the Control Test target number by his Sensor Rating and any analyze utility he is running. However, the test target number may not drop below 2, regardless of the decker's combined Sensor and analyze utility ratings.

Analyze Security

Test: Control
Utility: Analyze
Action: Simple

The Analyze Security operation tells the decker the current Security Rating of the host, the decker's security tall on the host (including any tally points accrued by the test for Analyze Security), and the host's alert status.

Analyze Subsystem

Test: Targeted Subsystem
Utility: Analyze
Action: Simple

An Analyze Subsystem operation identifies anything out of the ordinary about the targeted subsystem. The operation identifies the presence of scramble IC program or other defenses or system tricks present on the subsystem.

Control Slave

Test: Slave
Utility: Spoof
Action: Complex

The Control Slave operation enables a decker to take control of a remote device controlled by the host's Slave subsystem. Remote devices range from simple automatic security doors and elevator to entire automated factories full of robotic assemblers.

If the decker is attempting to take control of a manufacturing or scientific process controlled by the Slave subsystem, he must make the System Test with the average of his ratings in Computer Skill and a B/R or Knowledge Skill that applies to the process.

The Control Slave operation is a monitored operation.

Decrypt Access

Test: Access
Utility: Decrypt
Action: Simple

The Decrypt Access operation defeats scramble IC programs guarding access to a host. IC programs on a scrambled SAN must be defeated with a Decrypt Access operation before a decker can perform a Logon to Host operation on a scrambled SAN.

Decrypt File

Test: Files
Utility: Decrypt
Action: Simple

The Decrypt File operation defeats scramble IC programs on a file. Deckers must perform successful Decrypt File operations on scrambled files before performing other operations on such files. A file with scrambled IC programs cannot be downloaded until after it has been decrypted.

Decrypt Slave

Test: Slave
Utility: Decrypt
Action: Simple

The Decrypt Slave operation defeats scramble IC programs on a Slave subsystem. A decker cannot make Slave Tests against a scrambled Slave subsystem until he has performed a successful Decrypt Slave operation on the subsystem.

Download Data

Test: Files
Utility: Read/Write
Action: Simple

The Download Data operation copies a file from the host to the decker's cyberdeck. The data moves at the deck's I/O speed. It may be transferred to active memory, storage memory, or even off-line storage.

The Download Data operation is an ongoing operation that continues until the data transfer is completed, the decker logs off or is crashed, or the decker terminates the download early. If the operation is terminated before the transfer is completed, it crates a corrupted copy of the file, which is worthless.

However, if the file contains information that is particularly important to an adventure, the gamemaster may allow partially completed downloads to produce damaged, yet readable file copies. The base time to reconstruct a damaged file is calculated as follows: (full file size in Mp divided by amount of data downloaded in Mp) x 2.

The result is in days. Once a damaged file is reconstructed, the gamemaster determines whether the file contains the pertinent information by dividing the size of the downloaded file by the full size of the original file.

For example, if a decker manages to copy 10 Mp of a 100 Mp file, the base time for reconstructing the file is 20 days. Dividing 10 by 100 yields .10, so there is a 10 percent chance that the copied file contains the pertinent information.

Edit Slave

Test: Files
Utility: Read/Write

Action: Simple

The Edit File operation enables a decker to create, change or erase a datafile. Small changes (approximately one line of print or the equivalent of one short form of some kind) can be made directly on the host by performing this operation. Before replacing larger amounts of data, the decker must prepare the new material off-line first, then upload it and perform an Edit File operation to insert it into the file. Any uploaded information may be inserted with a single Edit File operation, regardless of its size.

A successful System Test creates new files. Because these files have counterfeit headers, the operating system ay notice irregularities.

Deckers also can use Edit File operations to make copies of tiles on the same host, Thus, deckers can copy a file from a particularly secure datastore, stash it on a less secure part of the same host and retrieve it at a later time. When using the Edit Tests. The first test is a Files Test. The second test is made against the subsystem that controls the location where the decker hid the copied files.

After altering, inserting, or deleting a file, a decker may make a Control Test, with target number reduced by his read/write utility, to authenticate the file's headers. Note the number of successes. If the decker fails to successfully take this step, make a Masking (Files) Test. The number of successes is the number of hours before the host notices the tampered file and reports it to the host's supervisor.

Deckers may also check to determine whether a file has been tampered with. If the file was altered by an unauthorized decker who failed to make a Control Test to authenticate the headers, then a simple Files Test will reveal the tampering. If the file headers were authenticated, the Files Test must achieve more successes than the tampering decker achieved on the Control Test to recognize signs of tampering in the file.

Keep in mind that nay time a decker deletes a host file, the gamemaster must consider the impact n the adventure in progress and decide whether back-up copies of the file exist.

Edit Slave

Test: Slave
Utility: Spoof
Action: Complex

This operation enables a decker to modify data sent to or received form a remote device controlled by the host's Slave subsystem. For example, a decker could perform Edit Slave operations to alter video signals or sensor readings from a computer-controlled security system or alter readings being sent to a console or simulator.

The Edit Slave operation is a monitored operation.

Graceful Logoff

Test: Access
Utility: Deception
Action: Complex

The Graceful Logoff operation enables a decker to disconnect from a host and the LTG where he logged on to the grid without experiencing Dump Shock.

In addition, a successful Graceful Logoff operation clears all traces of the decker and his actions from the security and memory systems of the host. A truck utility in its location cycle will add its rating as a target number modifier to any Graceful Logoff attempts.

Locate Access Node

Test: Index
Utility: Browse
Action: Complex

The Locate Access Node operation is basically "directory assistance". It enables a decker to find the codes to LTGs that provide access to the hosts he wants. The operation also lets him locate commcodes for regular telecom calls.

Modify the target number for the System Test according to the decker's stated goal. For example, if all he knows is a company or individual name – "I'm looking for a Mitsuhama system" – apply a +1 modifier to the target number. If his goal is a bit more specific – "I'm looking for a Mitsuhama public-relations system" – do not modify the target number. If he as a definite, specific goal – "I'm looking for the

Mitsuhama public relations system out of the Mitsu office in Bellevue on LTG 5209" – apply a –1 modifier to the target number.

Once a decker has located an LTG code, he need not repeat the Locate Access Node operation to find the host in the future – unless its owners change the address.

The Locate Access Node operation is an interrogation operation.

Locate Decker

Test: Index
Utility: Scanner
Action: Complex

The Locate Decker operation is a two-step process. The decker makes the standard System Test and then a Open-ended Sensor Test. The decker locates any other deckers whose Masking Attributes are equal to or lower than his Sensor Test results. In addition, he knows if they log off or jack out. If a targeted decker is running a sleaze utility, add its rating to the targeted decker's Masking Rating to determine if the testing decker locates the targeted decker.

Located deckers may break contact by maneuvering.

Friendly deckers who wish to make their presences known to each other may do so automatically.

Locate File

Test: Index
Utility: Browse
Action: Complex

The Locate File operation is an interrogation operation that searches for specific datafiles. To use the operation, the decker must have some idea of what is looking for – "valuable data" is not enough.

If the operation succeeds, the decker knows the system location of the file.

Locate IC

Test: Index
Utility: Analyze
Action: Complex

The Locate IC operation follows the same rules as the Locate Decker operation. However, the decker automatically locates the IC program(s) if his System Test succeeds – he need not make a Sensor Test. The IC program(s) remains located unless it maneuvers to evade detection.

Locate Slave

Test: Index
Utility: Analyze
Action: Complex

The Locate Slave operation follows the same rules as the Locate File operation. The operation is used to determine system addresses for specific remote devices controlled by the host. A vague inquiry would be, "Find all the security cameras controlled by this computer." A very specific inquiry would be, "Find the camera that monitors the eastern stairwell door on the third floor."

Logon to Host

Test: Access
Utility: Description
Action: Complex

The Logon to Host operation simply consists of the standard System Test. Apply any appropriate modifiers to the test and remember to begin counting the decker's security tally with any successes the host achieves.

The decker will not know the host's Access Rating until he takes his first crack at the logon. At that point, the rating will be all too evident. No need to make it a big secret.

Once the decker succeeds at the System Test, the virtual landscape of the computer becomes visible. If the decker is accessing a host directly through a workstation, his icon may appear in scenery corresponding to an I/O port. Of course, with the preponderance of sculptured systems in the Matrix today, the scene may be something quite unique.

Gaining access to a host through a remote device means the decker's icon enters the host at a slave controller, and access through the console puts the decker in the heart of the CPU node.

Logon to LTG

Test: Access
Utility: Deception
Action: Complex

The Logon to LTG operation simply consists of the usual System Test using the Access Rating of the LTG. If the decker loses the test, his logon attempt fails. The decker can try again, but is security tally remains on the grid for some time. The decker also can switch to a different jackpoint before his next logon attempt – which means the grid will have to start a new security tally for him.

Once the decker succeeds in the Success Contest, his icon appears in the familiar virtual landscape of the LTG. From an LTG, the decker can log on to the RTG that controls the LTG, or on to the PLTG attached to this LTG (if he knows its address), or to any host attached to the LTG (if he knows the host's address).

Logon to RTG

Test: Access
Utility: Deception
Action: Complex

Once he has logged on to an LTG, a decker can log on to its controlling RTG by performing a Logon to RTG operation. He must perform this operation if he wants to connect to a different LTG on the same RTG, or to a different RTG altogether.

To perform the operation, the decker makes a System Test against the RTG's Access Rating.

Once the decker is on the RG, he can perform a Logon to LTG to reach any LTG attached to the RTG, or a Logon to RTG operation to reach any other RTG in the world.

Make Comcall

Test: Files
Utility: Commlink
Action: Complex

A decker on an RTG can make a call to any commcode on an LTG controlled by that RTG performing a Make Comcall operation. But this operation is not just a way to beat payphones. The decker can make a call, then move to another RTG and make a call to a number under its control, then link the two together. A decker can move to multiple RTGs in this manner, building a secure conference call. Each call the decker lings together requires a System Test.

Deckers can be licensed to provide this service on various RTGs. This means they gat a passcode from the RTG vendor that authorized this operation. In that case, no tests are needed to make the calls or link them together. This license is usually restricted to corporate deckers.

The Tap Comcall operation cannot trace this kind of call, but another decker could use the track utility to try to locate the commcodes involved in the call.

In addition, the decker can detect any taps or tracers on the commlines by winning an Opposed Sensor versus Device Rating Test. He can neutralize them with another Opposed Test, pitting Evasion against the Device Rating.

Dumping a participant from a comcall requires a Files Test. Likewise, jumping into a tapped comcall requires a Files Test.

Deckers often arrange secure calls as a profitable sideline. The typical charge is 100 nuyen per caller per minute.

The Make Comcall operation is a monitored operation.

Monitor Slave

Test: Slave
Utility: Spoof
Action: Simple

This operation enables the decker to read data transmitted by a remote device. He can listen to signals from audio pickups, watch feeds from security cameras, examine readouts on a computerized

medical scanner hooked up to the host, and so on. As long as he maintains the operation, he receives constant updates from the device.

The Monitor Slave operation is a monitored operation.

Null Operation

Test: Control
Utility: Deception
Action: Complex

The gamemaster may require a decker to perform one or more Null Operation whenever the decker is waiting for something to happen, whether it is an event on the Matrix, the end of an ongoing operation, or something else that involves hanging around in cyberspace without making System Tests. The gamemaster may also call for a Null Operation if a decker is doing anything that requires actions but no System Tests, such as maintaining an Edit Slave. The gamemaster may secretly perform these operations on behalf of the decker, if he so desires.

Use the host's base Security Value for the Success Contest. If the decker is inactive on the host for less than 10 seconds. If the period of inactivity is less than a minute but more than 10 seconds, apply a +1 modifier to the Security Value. If the period is less than an hour but more than a minute, apply a +2 modifier. If the period is less than 12 hours but more than 1 hour, apply a +4 modifier; apply an addition +1 modifier for every additional 12 hours. The gamemaster may set an upper limit on the inactive period, depending on the decker's ability to avoid falling asleep in the event of such implausibly long times.

If the Security Test raises the decker's security tally and triggers a response from the host, the gamemaster should activate the response as he sees fit, perhaps after a percentage interval of the decker's period of inactivity.

Swap Memory

Test: None
Utility: None
Action: Simple

The Swap Memory operation enables a decker to load a new utility program into his deck's active memory and then upload it to his on-line icon.

Loading the utility to active memory is a Simple Action – the decker simply tells the decks to do it. If his deck does not have enough active memory to hold the new program, he must first spend a Free Action to unload a program from his deck's active memory. No tests are required for these actions.

Once the utility is in active memory, it automatically start uploading to the icon.

Tap Comcall

Test: Special
Utility: Commlink
Action: Complex

The Tap Comcall operation enables deckers to locate active commcodes on an LTG, trace and tap commcalls. Deckers use the commlink utility for all the tests required during this monitored operation.

To locate active commcodes on an LTG, a decker must be active on an RTG that controls the LTG. The decker makes an Index Test to determine if any commcodes on the LTG are sending or receiving a call. If the decker is checking for a particular commcode, he must be on that commcode's parent RTG, and he receives a –2 target number modifier for the Index Test. If the decker finds a commcode n use, he can make a Control Test to trace the call to its origin or destination. If multiple participants are undertaking a conference call with that commcode, each net success on the test reveals the commcode of one participant.

If the call was set up by another decker using the Make Comcall operation, then the Control Test locates the decker controlling the call. The decker trying to trace the call must move to the RTG the calling decker is currently located in and use a track utility against him. Note that using the track utility on a decker is considered an attack and reveals your presence to that decker. The track utility locates all other commcodes involved in the call.

If the decker wants to tap the call and record it in his deck's storage memory or off-line storage, he must make a Files Test. Each minute of recording occupies 1 Mp of storage.

If the comm connection is scrambled, the decker must decrypt it by making an Opposed Test by pitting his Computer Skill against the Device Rating of the data encryption system on the comm. line. The decrypt utility reduces the decker's target number. If the first decryption test fails, the decker can try again; apply a +2 modifier to the target number for each additional test. None of the tests against scrambling affect the decker's security tally on the RTG.

If any of the phones involved in the call are equipped with a dataline scanner, the decker may that off even if he doesn't trigger an alert on the RTG. Dataline scanners have a rating from 1 to 10. Once the decker establishes his tap, the decker must make an Opposed Test, Computer Skill versus the scanner's Device Rating. The commlink utility reduces the decker's target number. If the decker wins, he has synchronized the tiny fluctuations in signal integrity cased by his tap and fooled the scanner. If multiple dataline scanners are in use on the call, use the highest rating among them for the test. In this case, the decker needs 1 success for each scanner involved, or some of the devices detect the tap. Whether this test succeeds or fails, the result does not affect the decker's security tally on the RTG.

Once a decker has tapped and unscrambled a call, he can listen in and record as he wishes. When the call terminates, he cal stay locked on to any of the commcodes, either the original one that he was after or any that he traced. He can then attempt to monitor any subsequent calls placed from the commcode. If the decker is monitoring a code that he has already tapped, he does not need to make Index Tests to determine when it becomes active again. He does need to make new tests to trace or tap the new calls and defeat any dataline scanners or encryption on the calls.

Deckers may also reveal themselves and enter in tapped comcalls, or disconnect participants from comcalls by performing a Make Comcall Operation (Files Test, modified by commlink utility).

Tap Comcall is a monitored operation.

Upload Data

Test: Files
Utility: Read/Write
Action: Simple

This operation enables a decker to transmit data from his cyberdeck to the Matrix. This data comes directly from the deck's storage memory and does not affect active memory.

If the decker is creating a new file on the host, the file is written automatically. If the decker intends to modify an existing file on the host – adding false records to a database, for example – the decker must perform an Edit File operation after the upload is finished.

Note that the Upload Data operation is not used to upload utilities. The Swap Memory operation handles that function.

The Upload Data operation is an ongoing operation.

Appendix B
Decker Utilities

Operational Utilities

Operational utilities help deckers execute system operation, in the same way that a samurai's smartlink makes his gun a more effective tool and his dermal armor backs up his armored jacked. Operational utilities reduce the target numbers of a decker's System Tests by the utility rating. Deckers may perform system operations without utilities – not having the right program does not make the operation impossible, just more difficult.

Analyze

Multiplier: 3
System Operations: Analyze (Host, IC, Icon, Security, Subsystem), Locate IC

The analyze utility reduces the target numbers for System Tests that identify IC, programs and other resources or events controlled by a host.

Browse

Multiplier: 1
System Operations: Locate Access Node, Locate File, Locate Slave

The brose utility reduces the target numbers of Index Tests made to locate specific data values or system addresses. Unlike analyze and scanner utilities, which search for Matrix activity, the browse utility works on the contents, or real-world functions, of these data nodes.

Commlink

Multiplier: 1
System Operations: Make Comcall, Tap Comcall

The commlink utility reduces the target numbers of any tests that affect the decker's communications links.

Deception

Multiplier: 2
System Operations: Graceful Logoff, Logon to (LTG, RTG, or Host)

Unless otherwise noted, the deception utility may be used to reduce the target number of all Access Tests.

Decrypt

Multiplier: 1
System Operations: Decrypt Access, Decrypt File, Decrypt Slave

The decrypt utility reduces the target numbers of any System Tests made to defeat scramble IC programs.

Read/Write

Multiplier: 1
System Operations: Download Data, Edit File, Upload Data

The read/write utility reduces the decker's target number for System Tests necessary to transfer files or otherwise access, edit, or create data in the Matrix

Relocate

Multiplier: 2

This utility is used against track utilities in their location cycle. The decker using relocate engages the tracking decker in a Success Contest. The relocating decker makes a Computer Test, with a target number equal to his opponent's Sensor Rating minus the Relocate Utility Rating. The tracking decker makes an MPCP Tests against the Relocate Utility Rating. If the relocating decker wins, the track program

fails completely. The attack must successfully attack the target decker again before using the track utility against his opponent.

Scanner

Multiplier: 3
System Operations: Locate Decker

The scanner utility reduces the target numbers of System Tests made during operations that search for deckers.

Spoof

Multiplier: 3
System Operations: Control Slave, Edit Slave, Monitor Slave

The spoof utility reduces the target numbers for all System Test made to affect systems and subsystem slaves.

Special Utilities

Special utilities perform specific jobs that fall outside the standard utilities, such as offensive or operation utilities.

Sleaze

Multiplier: 3

The sleaze utility combines with a deck's Masking Rating to enhance the decks' Detection Factor: (Masking + Sleaze) / 2, round up.

Track

Multiplier: 8

The track utility is a trace program used as a combat program against hostile deckers. After each successful attack, note the number of successes the attacking decker scored. The target decker must make an Evasion (Track Rating) Test. If the Evasion Test fails to yield an equal or greater number of successes, the attacker's track utility locks onto the target decker's datatrail and begins its location cycle. Divide 10 by the attacker's net successes to determine how many turns the track utility needs to locate the target decker's jackpoint.

For the purposes of measuring the location cycle, only count full Combat Turns. If a decker can freeze or destroy the IC before the last Initiative Pass of a Combat Turn is completed, that turn is not considered completed.

The target decker can try to escape the attacking decker by logging off or jacking out. However, the track utility makes logoff operations more difficult.

Targeted deckers can use the relocate utility against track programs. Of course, the target decker can always crash the attacking persona, which would stop all its pesky programs.

Offensive Utilities

Offensive utilities inflict damage on the icons of deckers, IC programs, running programs, datafiles – pretty much anything. Some offensive utilities, such as the attack utility, are general, brute-force destructive viral logics. Others are subtler and more limited. The following descriptions specify the targets each utility program can attack.

Attack

Multiplier
Light: 2
Medium: 3
Serious: 4
Deadly: 5
Target: Personas, IC

The attack utility, the least subtle offensive program, can be programmed to inflict Light to Deadly damage. It sample the instruction algorithms of the targeted icons and tries to introduce fairly coarse

memory faults into the icon's most frequently accessed code segments. In cybercombat, that translates to a direct attack on the Condition Monitor of the decker's persona or IC icon.

The attack utility affects on-line icons only and has no effect on a decker's meatbody or cyberdeck. The armor utility reduces the Power of damage done by attack utilities.

Black Hammer

Multiplier: 20
Target: Deckers

Five years ago it was a rumor, four years ago a bleeding-edge weapon on the decks of Lone Star's GridSec elites. Three years go the so-called black hammer utility began cropping u in shadowy hands and today it is a standard offensive utility that most deckers take for granted.

The black hammer utility is a black IC program that targets the decker, not the deck. I can kill a decker without knocking his cyberdeck off-line, so that the decker's jackingpoint remains traceable. Black hammer lacks the blaster-like capabilities of mainframe-drive black IC, but otherwise its effects are identical to those of lethal black IC.

Killjoy

Multiplier: 10
Target: Deckers

The killjoy utility mimics non-lethal black IC. Killjoy programs inflict Stun damage to a decker's meatbody. Otherwise, the killjoy utility is identical to the black hammer utility.

Slow

Multiplier: 4
Target: IC

The slow utility reduces the execution speed of proactive IC. Whenever a decker attack IC with the slow utility, make an Opposed Test, pitting the Security Value against the Slow Rating. If the IC generates more successes, nothing happens to it. If the slow achieves more successes, the IC loses 1 action for every 2 net successes the slow achieved. If the IC has no action left in a turn, it hangs – goes dead.

Note that temporarily disabling IC in this manner prevents the IC from raising the decker's security tally. However, suppressing the IC requires 1 point of Detection Factor. If the IC is not suppressed at the beginning of the next Combat Turn, the gamemaster rolls initiative for the IC per standard rules and the IC resumes where it left off.

Reactive IC is not vulnerable to the slow utility.

Defensive Utilities

Defensive utilities are designed to prevent, reduce, or repair damage taken in cybercombat. As with offensive utilities, add or subtract the utility rating as indicated in the individual descriptions.

Armor

Multiplier: 3

The armor utility reduces the Power of damage inflicted on a decker's icon by the Armor Rating. For example, the armor utility reduces damage caused by killer IC or the attack utility. Against black IC, armor only reduces the Power of damage taken by the decker's icon – not damage taken by the decker's meatbody. In short, the armor utility is always effective against standard damage to the icon's condition monitor but has no effect on collateral damage to the decker or his deck, which must depend on Hardening for protection.

The armor utility loses 1 Rating Point every time the decker takes damage – every time it fails to completely absorb damage from a hit. Deckers can replace degraded armor utilities with fresh copies of the program by performing the Swap Memory operation.

Cloak

Multiplier: 3

The cloak utility reduces the target numbers for Evasion Tests made curing combat maneuvers.

Lock-On

Multiplier: 3

The lock-on utility reduces the target numbers for opposed Sensor Tests made during combat maneuvers.

Medic

Multiplier: 4

The medic utility is used to reduce the number of filled-in boxes in the on-line icon's Condition Monitor. To use the utility, a decker must spend a Complex Action and make a Success Test using a number of dice equal to the medic utility's rating. The target number is determined by the level of damage the icon has suffered, as shown on the Medic Target Numbers Table.

Each success achieved on the Success Test repairs 1 would on the icon's Condition Monitor. The program loses 1 Rating Point each time it is used, whether it scores any successes or not. Deckers may load a new copy of the medic utility at its full rating by performing a Swap Memory operation.

Appendix C
Decker Tables

Stock Cyberdeck Types

Allegiance Sigma	Rating: MPCP-3 Active Memory: 200 I/O Speed: 100 Cost: 14,000	Hardening: 1 Storage Memory: 500 Response Increase: 0
Sony CTY-360-D	Rating: MPCP-5 Active Memory: 300 I/O Speed: 200 Cost: 70,000	Hardening: 3 Storage Memory: 600 Response Increase: 1
Novatech Hyperdeck-6	Rating: MPCP-6 Active Memory: 500 I/O Speed: 240 Cost: 125,000	Hardening: 4 Storage Memory: 1000 Response Increase: 1
CMT Avatar	Rating: MPCP-7 Active Memory: 700 I/O Speed: 300 Cost: 250,000	Hardening: 4 Storage Memory: 1400 Response Increase: 1
Renraku Kraftwerk-8	Rating: MPCP-8 Active Memory: 1000 I/O Speed: 360 Cost: 400,000	Hardening: 4 Storage Memory: 2000 Response Increase: 2
Transys Highlander	Rating: MPCP-9 Active Memory: 1500 I/O Speed: 400 Cost: 600,000	Hardening: 4 Storage Memory: 2500 Response Increase: 2
Novatech Slimcase-10	Rating: MPCP-10 Active Memory: 2000 I/O Speed: 480 Cost: 960,000	Hardening: 5 Storage Memory: 2500 Response Increase: 2
Fairlight Excalibur	Rating: MPCP-12 Active Memory: 3000 I/O Speed: 600 Cost: 1,500,000	Hardening: 6 Storage Memory: 5000 Response Increase: 3

Medic Target Numbers Table

Wound Level	**Target Number**
Light	4
Moderate	5
Serious	6

Program Size Table

Program Rating	Multiplier									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	2	3	4	5	6	7	8	9	10
2	4	8	12	16	20	24	28	32	36	40
3	9	18	27	36	45	54	63	72	81	90
4	16	32	48	64	80	96	112	128	144	160
5	25	50	75	100	125	150	175	200	225	250
6	36	72	108	144	180	216	252	288	324	360
7	49	98	147	196	245	294	343	392	441	490
8	64	128	192	256	320	384	448	512	576	640
9	81	162	243	324	405	486	567	648	729	810
10	100	200	300	400	500	600	700	800	900	1,000
11	121	242	363	484	605	726	847	968	1,089	1,210
12	144	288	432	576	720	864	1,008	1,152	1,296	1,440
13	169	338	507	676	845	1,014	1,183	1,352	1,521	1,690
14	196	392	588	784	980	1,176	1,372	1,568	1,674	1,960

Overload Damage Target Numbers

Icon Damage Level	**Target Number**
Light	2
Moderate	3
Serious	5

Dump Shock Damage Levels

Host Security Code	**Damage Level**
Blue	Light
Green	Moderate
Orange	Serious
Red	Deadly