

## V. Netrunning

### Navigating the Net

First step before hacking into a system is to locate it inside the matrix. This is done by a location roll. If system is generally accessible a simple Networks roll will do the trick to locate it. If system is hidden it will require social engineering (talking to people on forums, meeting contacts, stealing the information from somebody who might know...) or follow a trail of data (system knowledge). Ultra secured systems are not connected to the web at all. They must be accessed physically. Locating them is same as hidden systems, just more difficult.

The following chart indicates the difficulty (TN) to locate a system inside the matrix:

Security Level	Description	Dif.
1	Unsecured	0
2	Low security	-1
3	Medium security	-3
4	Top notch security	-6
5	High security	-9
6	Top secret	-12

#### Relevant skills:

Networks	This is used to search via search engines, crawlers...
System knowledge	Used to search by following the trail of an e-mail or phone call...
Streetwise	Used to search by using forums, asking contacts...

### Intrusion Attempts

#### Hacking

To hack into a system, follow this procedure:

1. Hacker specifies the time he's going to spend on the intrusion attempt. Refer to the System Security Level chart above and to the Hacking Time Modifiers Chart below for bonus/penalty.
2. The hacker specifies if he uses a neural interface system (requires interface plugs and a cyberdeck) or not.
3. The hacker makes a (intrusion/security) check.

Time Spent	Keyboard	Neural Interface
1 action	-12	-6
1 round	-9	-3
5 minutes	-6	-1
15 minutes	-3	0
30 minutes	-1	0

1 hour	0	0
1 day	+1	+1
1 week	+3	+3
1 month	+6	+6

- ❑ Critical success means the hacker successfully penetrates the system much faster than expected (one step faster).
- ❑ Success means he gets inside in the specified time.
- ❑ Failure by 1 means the attempt failed, but no one is alerted. The hacker can try again by spending additional time.
- ❑ Failure by 2 means the attempt failed, but defenses are alerted. If the hacker tries again within 24h, there will be an extra -2 penalty. If the hacker was using a hole created through icebreaking (see below), that hole is closed and the system's security level returns to full strength against both the hacker and anyone else that had hoped to rely on the same hole.
- ❑ Failure by 5+, or critical failure, has the same effect, and triggers any active countermeasures.

### Probing Attempts

Instead of trying to break in immediately, a hacker can take time to carefully probe a system's defenses. A probe attempt is treated like an intrusion attempt with the exception that the hacker suffers no Security Level penalty.

- ❑ Critical success means he discovers the system's security level and finds a possible back door that will give him a +3 bonus on any break-in attempt.
- ❑ Success means he discovers the security level.
- ❑ Failure means no useful information is found but the hacker can try again by spending more time.
- ❑ Failure by 5+, or critical failure, means the target is alerted (see above): hackers suffer -3 on all hacking attempts in the next 24h.

*Note on backdoors: Backdoors don't need to be used right now. They can be used at any time by anybody as long as nobody failed completely his hacking attempt.*

### Icebreaking

A hacker faced with very powerful defenses may try to attack the systems security instead of trying to bypass it. This is referred to as "icebreaking". Icebreaking requires a (intrusion/security) skill check and the usual time. The security level is reduced by one level.

- ❑ Critical success means the hacker has found a fatal flaw and completely subverted the security system. Any intrusion attempt will automatically succeed.
- ❑ Success means that the hacker has subverted part of the defenses: the security level drops by one against his next icebreaking or intrusion attempt. If desired the hacker can keep trying, with each success further reducing the defenses (to a minimum of 0).
- ❑ Failure by 1 means the attempt failed, but no one is alerted. If this was a repeated attempt to enlarge an existing hole, the original hole is not detected and the defenses remain weakened.
- ❑ Failure by 2 means the attempt failed, and the defenses are alerted. Any hole the hacker has

previously opened is now closed, and the security level returns to full strength.

- Failure by 5+ has the same effect but triggers any active countermeasures.

*Note: holes can be passed to other hackers, which can be exploited as well – at least, until one hacker fails an icebreaking or intrusion attempt by 2+, which will close the hole to everyone.*

## 1. Inside the System

Once a hacker has accessed a computer system either via stealing the password or a successful intrusion, he can perform all kinds of mischief and mayhem. These activities are less likely to be detected: usually only a critical failure will trigger active counter measures.

### Manipulating Data

The hacker can try to locate information stored on the system by checking through directories or running search programs. This requires a Databases skill check. Add bonuses for the desired time spent (see Table for hacking time). Additional modifiers depend on how much data the computer system holds, from +1 (a few files) to -9 (a massive library of data). Critical success means the hacker serendipitously finds exactly what is being sought, or possibly stumbles on other useful files.

- Success means a hacker who knows what to look for finds that particular file, or discovers its absence with certainty. If the hacker is snooping about, a success means the GM can provide a sense of what is available (perhaps a list of directories, like “Research Division Personnel Files,” “Members-Only VR Access,” or “Project Nemesis Test Results”). The hacker can further refine the search based on this (and another Skill check).
- Failure means he or she does not find anything helpful, but can try again by spending more time.
- A critical failure means that the hacker’s inquiries were deemed suspicious and Active Countermeasures were triggered (see below). Once located, data files can be copied, read online, moved, or deleted. Each attempt usually takes only one round (but reading or copying a huge file may take longer). No Skill roll is usually necessary to perform the operation, but a successful Databases skill check must be made to do so without alerting security.

### Virus, System crashing, and other Sabotage

A hacker can try to crash the computer that controls the system he or she has infiltrated. This requires a Networks skill check at a -3 penalty. Each attempt takes one round; there are no time modifiers.

- Failure and critical failure have the usual effects.
- Success means the system goes down. This will alert any humans (or A.I.s) who were using the system, but also shut down all computer-controlled systems run by it. The hacker is automatically kicked offline. Unsaved data being worked on will be lost, and a lot of people will be aggravated.

### Rebooting the Network

The system operator will need to reboot the system, perform security checks, and restore files. The system’s operator requires a Networks check to get it back online (roll every 10 minutes) at a penalty equal to the amount by which the hacker succeeded. For example, if the hacker

succeeded with a roll of 8, the system operator would roll at -8 to bring the system back on line.

### Viruses and hidden Programs

A more subtle way to sabotage a system is to insert a virus or other hidden program into the target computer. It can be set to trigger at a later date or if a specification is performed, such as an attempt to use the system against the hacker or his or her friends. It might be set to periodically mail out new data files to the hacker (acting as a spy), crash the system, or even erase data. An example of a subtle buried program would be one that altered or erased all references to a particular person after they were uploaded.

Creating a virus requires a Programming skill check. Difficulty depends on the virus' ability (0 annoying program to -12 Stuxnet-like).

### Detecting hidden Programs

System operators may detect a buried program. Use the Manipulating Data rules (chapter 3.1) to see if the system operators notice it, rolling every day if the program is active (if it's operating constantly, grant them a +3 bonus), or less frequently (for example, whenever they do a major security check, such as monthly) if it is a buried "time bomb." If they find it, they will erase it and try to locate the intruder. Erasing a buried program requires a Programming skill check made at a penalty equal to the Programming skill Level of the character who buried it.

### Controlling computerized Devices

A system may include programs that run devices such as electronic doors, vending machines, automated factory or lab equipment, security cameras, or even teleoperated robots. The file containing the program that controls a particular system can be located using the rules for Manipulating Data (chapter 3.1). Once it has been found, the hacker can try to control it. This requires an Intrusion/Security skill check; the usual time modifiers for hacking apply. Success means the hacker has taken over that system. Failure means he did not but can try again, while critical failure alerts defenses. A hacker will usually only be able to control one such system at a time. Each extra system he or she tries to control simultaneously imposes a -3 penalty on all checks. Teleoperated systems such as automated weapons or robots may require other Skills to use properly. Thus, if the character takes over an automated factory unit, he or she will need appropriate Electronics or Mechanics Skill to tell the unit how to build something (or hack into the databases to find an existing program).

## 2. Security Level

A computer system is rated for its Security Level, from 1 (fairly lax) to 6 (ultra-tight). This is a combined rating that takes into account defense programs, virus protection, hardware security, and the alertness of users and system operators to threats.

Security Level	Description	Dif.	Example
1	Unsecured	0	Technically impaired neighbors
2	Low security	-1	High school, small business, or private VR club
2	Medium security	-3	Hospital, university, local government office
4	Top notch security	-6	Large corporate or federal government or minor criminal enterprise
5	High security	-9	Megacorporate R&D server or major criminal data haven
6	Top secret	-12	Major bank or government intelligence agency

## Active Counter Measures

Basic security programs keep people out, but some security systems are more like watchdogs than locks. Active Countermeasures are programs that counterattack the hacker. They are triggered under the following circumstances:

- An intrusion or icebreaking attempt that fails by 5+ (or is a critical failure).
- A critical failure while engaged in any activities inside the system

Systems may have one or more of the following Active Countermeasures. Neural Feedback and Mind Trap are only available on systems with Security Level 4+. The GM can come up with other Countermeasures, or may permit hackers to use Computers (Programming) Skill to design new types of programs.

### Tracer

This program pretends to accept the hacker, but feeds false or inconsequential data while attempting to “back trace” to discover the hacker’s real computer address.

The hacker gets an Intrusion/Security skill check to notice and block or misdirect the trace. No time modifiers apply, but a -3 penalty applies if not using a neural interface. Apply an additional penalty equal to the system’s Security Level.

Success means the trace has been blocked for one round. If the hacker were trying to gain access, he or she can simply log off. If the attacker was inside the enemy system, he or she has the option of either logging out (and thus eluding the trace) or taking an extra round to perform some sort of action. Note that actions performed in a single round will suffer a -3 time penalty (-6 if not using a neural interface).

Failure means the trace was not blocked, and the program discovers the general “address” of the hacker’s system — what server he or she was using. The consequences may vary, from a warning email, to a visit by men in black suits the next day, to an orbital satellite strike, depending on exactly what the character was trying to hack into.

### Neural Feedback (Black Ice)

This program only affects hackers who are using neural interfaces. It launches a counter-attack, reaching out across the net to override the hacker’s nervous system (if he or she is using a neural interface headset or neural jack). This works like a Tracer program (above), except that if the hacker fails the check, he or she suffers neural feedback. That is, the hacker takes 2d6 damage, ignoring any ordinary armor or defenses. It will continue to inflict damage each round, if it can. When it is the hacker’s turn to act, he or she may attempt to break free by logging out. This would normally be simple (just hit “power off” or remove the jack or neural headset ‘trodes), except that the damage inflicted is often enough to inflict KO on a failed CON+Endurance check. Careful hackers will often have a partner standing by to jack the hacker out of the system if he or she is stunned or knocked out. The victim will still take the first 2d6 damage, but the damage will not continue.

A Neural Feedback program requires in most countries a government license (only available with Security Levels 4+).

## **Mind Worm**

This is the most insidious form of defence program; in some settings, it may be beyond available technology, merely a hacker's urban legend.

Mind Worm functions like Tracer except that if the user fails to block it and possesses a neural interface, it infiltrates his or her cyberbrain. Treat this as COOL vs. COOL combat. The Mind Worm program has an effective average COOL equal to its Security Level x2. The target may add his or her Resist Torture/Drugs skill level to his or her Mind before averaging it with COOL. As usual, the target must make a Stat check at -6 to break away. If the Mind Worm cracks the target's mind, it may "brain hack" his or her memories, plant suggestions, and so on, as detailed under *Mind Combat (define that)*, depending on what it was programmed to do. In some settings, it may be possible for a Mind Worm to actually brain scan the subject and store a mental duplicate of him or her in a virtual reality — effectively "trapping" the victim in cyberspace. If the hacker wins, he or she has destroyed the Mind Worm program and, in addition, is treated as having gained a critical success with an icebreaking attempt (see above).

Ideas: Firewall of different levels to prevent cyberbrain hacking. Surges to avoid fatal feedbacks and destroyed cyberdecks.

(This part could need some improvement)