that eliminating the access ID entirely is not an option, as most nodes will refuse access to unidentified devices; access ID must be spoofed instead.

Hackers & Editing

Note that many hackers use their Edit program to eliminate any records of their tampering or illicit activity on a node. To do this, the hacker first needs to locate the node's security logs (requiring a Data Search action), and then edit them to remove all traces of his activity.

Depending on your account privileges, Edit may also be used to create, change, or delete accounts on a particular node. Hackers are fond on making back doors (hidden accounts) into systems they have hacked this way, so they can get inside later with having to hack in again. Edit may also be used to alter subscription lists (see *Linking and Subscribing*, p. 212).

Use Hacking skill + Edit for unauthorized file tampering.

USING ELECTRONIC WARFARE SKILL

Electronic Warfare pertains to the use of communications technology, from wireless devices to cryptography. Want to locate someone's hidden PAN? Break the encryption on a drone's system? Jam a corporate strike team's communications? Electronic Warfare is the skill for the job.

When dealing hands-on with communications technology, make tests using Electronic Warfare + Logic. When utilizing programs, use Electronic Warfare + program rating.

Electronic Warfare skill plays a particular role in the following Matrix actions.

Detecting Wireless Nodes

Locating a particular active or passive wireless node within range (or all of them, for that matter) takes only a Free Action, no test required. Commlinks routinely scan for new nodes, so finding one is just a matter of looking it up. Finding a particular node in a crowded area might be more difficult: make an Electronic Warfare + Scan (variable, 1 Combat Turn) Extended Test against a gamemaster-determined threshold based on the difficulty of finding and selecting out the node in question.

Finding a wireless node in hidden mode (see p. 211), however, is more challenging. Even if you know what you're looking for, you must still succeed in an Electronic Warfare + Scan (4) Test. If you're just scanning for hidden nodes in general, or trying to pick the hidden nodes out from the non-hidden one, make the same Extended Test noted above but with a much higher threshold: 15+.

Encryption and Decryption

Files, signals, and devices may all be encrypted with a Simple Action . If you have the proper key, decrypting takes only a Simple Action. Without a key, you must employ a battery of advanced sampling, pattern-matching, and brute-force attacks to bypass the encryption. Make a Decrypt + Response (Encryption rating x 2, 1 Combat Turn) Extended Test to break the encryption.

Note that some encryption schemes may incorporate IC as a second line of defense.

Intercepting Wireless Signals

Wireless traffic is broadcast through the air, so anyone within range of a signal can pick it up, whether they are connected to the transmitting party or not. Thus you can eavesdrop on the wireless connections of anyone whose Signal range reaches you. This makes it possible for you to even intercept traffic within a specific network—such as the PAN traffic between Mr. Johnson's commlink and other devices on his network.

To perform an Intercept Wireless Signal action, make an Electronic Warfare + Sniffer (3) Test. Once the signal is intercepted, you can monitor the traffic and even copy/record/forward it without making any more Intercept Wireless Signal actions. If you want to block out some parts of the traffic or add in your own, you must make an Edit action.

There is no way to detect interception of a wireless signal.

Note that wireless communications are usually encrypted, so you'll need to decrypt the signal *before* you can intercept or capture the traffic.

Jamming

Jamming—also known as electronic countermeasures—requires special hardware that is heavily restricted (see p. 320). Jammers come in two varieties: area jammers and spot jammers. Area jammers broadcast over a large area (based on their Signal attribute), effectively blanketing out all wireless nodes in that area. Spot jammers concentrate their jamming in a narrow angle, which makes them very effective against individual targets. Jammers are opposed by electronic counter-countermeasures (ECCM), which filter out jamming signals. Jamming a wireless node cuts off its Matrix connection unless it is hardwired to a Matrix gateway.

Initiating jamming is a Complex Action. Any device with a Signal rating less than the jamming device's Signal rating is overwhelmed. Note that ECCM (see p. 227) increases a protected device's Signal rating for jamming comparison purposes.

Note also that jamming can be either selective (targeting specific frequencies) or a barrage attack that seeks to interfere with all frequencies.

PROGRAMS

Programs are the software tools that you use to make things happen in the Matrix. Programs come in many types: Attack programs for demolishing icons, Exploit programs to hack in to a protected system, Armor programs to protect against Matrix attacks, Browse search routines to locate the hottest paydata, and so on.

Programs have variable ratings, normally in the range from 1 to 6, though some cutting-edge or military-grade software can rank higher. A program's rating is used to determine how effectively the program accomplishes its intended function.

Remember that a device cannot run a program at its full effect at a rating above its System rating (A Rating 5 program run on a System 3 device operates as if it were Rating 3). Additionally, if a device is running more programs at once than its System rating, reduce the Response on that device by 1 per (System) programs (ie, a System 5 device running 10 programs at once suffers –2 to its Response).