Urgent Message...

WHAT EVERY RUNNER NEEDS TO KNOW ABOUT HACKING

Any runner team that fails to practice good data security is going to get hacked. Just as the team's hacker can infiltrate Mr. Johnson's commlink, trace that snitch's access code, seize control of that police drone, or disable that assassin's smartlink, any hacker-aided opposition will seek to do the same to them. <Insert Evil GM cackle here.>

The first lesson is: any wireless device can be hacked. Cyberlimbs. Smartlinked guns. Commlinks. Drones. Cameras. Refrigerators. If it has an active wireless connection, it's vulnerable. You can always temporarily or permanently disable wireless features, but it may mean a substantial loss of functionality, putting you at a disadvantage.

The following security hints and tips are recommended to all denizens of the shadows, player character and NPC alike.

- **Don't advertise**—PANs have their uses, but they're also detectable. No covert ops team worth its rep is going to sneak up on a target with their PANs active—they'd be toast to anyone keeping an eye on the airwaves. Likewise, social networking might be a nice way to get a booty call, but runners should know better than to broadcast personal details that a snooper can use against them. Fake details, on the other hand ...
- **Limit your vulnerabilities**—Wireless devices are neat, but if they're not well protected, they're a hacker's next meal. If you need a device, beef up its IC (that's why hacker teammates and contacts are good to have). If you don't need it, turn it off.
- **Don't leave tracks**—Everywhere you or your PAN go, you leave a datatrail. That evidence can be used to pin you to a particular location at a particular time and in the vicinity of specific objects or people. Spoof your datatrail, or have a hacker do it for you.
- **Fake ID is your friend**—Even if active mode isn't required, running with a legit-looking ID might keep you from standing out in a crowd. Just don't rely on it for too long, or it might become a liability.

cessed. If you fail, the Data Bomb activates, inflicting Rating boxes of Matrix damage. Depending upon its settings, the Data Bomb may also trigger an alert and/or destroy the file it was protecting. Once defused, a Data Bomb program is inactive and no longer protects the file/device until it is restored.

Intercept Traffic

In order to intercept traffic between any two nodes or users, you must first have access to a node that the traffic passes through. For example, to intercept a comcall between a Mr. Johnson and his lackey, you either need to compromise one of their commlinks or gain access to the Matrix nodes that the comcall passes through (which could be a challenge unto itself). Note that this action only applies to traffic passing through a wired medium; for wireless traffic, see *Intercepting Wireless Signal,* p. 225. The gamemaster may also require you to succeed in a Computer + Browse Test to locate the traffic flow you seek to intercept.

To eavesdrop, make a Hacking + Sniffer Test. The hits you score are the threshold for anyone to detect your tap with a Matrix Perception Test. Taps of this nature are difficult to detect. In order for someone to detect interception of his wired traffic, he must make a Matrix Perception Test in the specific node on which the Sniffer program is running.

Intercepted communications can be copied/recorded without any additional tests. If the hacker wishes to block some parts of the traffic or add in his own, he must make a successful Computer + Edit Test (see *Edit,* p. 218). If the hacker wants to insert faked traffic, so that it looks like it comes from one party or the other, he must beat the recipient in an Opposed Test between his Sniffer + Hacking and the target's Firewall + System.

Note that some communications may be encrypted. In this case, a Decrypt action (p. 225) is necessary to capture and decode the traffic.

Redirect Trace

A Redirect action comes in handy when someone is attempting to trace your originating node (see *Track,* p. 219). By redirecting, you send a flurry of spoofed signals out in the hope of confusing the Track program. Each net hit scored on an Opposed Hacking + Spoof vs. Computer + Track (System + Track if launched by a node) adds 1 to the trace's threshold.

Note that you can only Redirect a trace in progress. You may take multiple Redirect actions against the same trace.

Spoof Command

Use the Spoof Command action to transmit forged instructions to an agent or drone controlled by another user. In order to spoof orders, you must first complete a successful Matrix Perception Test on the persona you are impersonating in order to gain its access ID.

To spoof commands, you must beat the agent or drone in an Opposed Test between your Hacking + Spoof and the target's Pilot + Firewall. If successful, the target drone or agent believes the orders came from its controlling persona. .

Spoofing the Datatrail

Most users are oblivious to invisible datatrail logging (see p. 216); hackers, however, prefer to eliminate such traces. Any hacker worth his name will either spoof his commlink's access ID on a regular basis; this requires a Hacking skill + Spoof program (2) Test. Alternately, you can modify the hardware itself to supply a bogus code with a Hardware + Logic (2) Test. Note