Issuing Commands

While online, you can issue commands to an agent (p. 227), drone (p. 238), sprite (p. 234), or other device under your control with a Simple Action. Note that you can issue the same command to multiple agents, drones, or sprites at once with the same action; different commands, however, require separate actions.

Note that agents and drones will only take orders from their controlling persona, unless another persona spoofs an order (see *Spoof Command,* p. 224). If the controlling character chooses, he can instruct the agent or drone to receive orders from other specified personas.

Reboot

A persona or node can shut down and reboot, but the process takes time. Make an Extended System + Response Test (10, 1 Combat Turn) to determine how long. Initiating a reboot is a Complex Action. A rebooted persona starts again in its personal node, not wherever it was in the Matrix when it rebooted.

Rebooting is more complicated for technomancers, as they cannot simply shut their brains off. In order to reboot, a technomancer must sever his Matrix connection completely and make an Extended Logic + Willpower Test (10, 1 hour) while fully resting (no physical, draining, or Matrix activity). After this recovery period has passed, the technomancer may reconnect to the Matrix with his living persona's attributes fully restored.

HACKING

No shadowrunning team can expect to get by for long without a hacker (or technomancer) on their side. Hacking is called for whenever you wish to manipulate the programming of computers and electronics—especially Matrix nodes—in ways that are not authorized.

Hacking is centered around defeating a node's firewall and breaking in. System security likewise focuses on employing intrusion countermeasures (see p. 228) to keep hackers out. If you successfully bypass security and infiltrate a node, that system will generally treat you as a legitimate user and will not challenge everything you do. You will need to stay alert so that you do not run afoul of security hackers and patrolling IC (see *Hacked!—Once Inside,* p. 222) or accidentally trigger an alarm (see *Intruder Alerts,* p. 222). If you raised an alert while breaking in, however, then the system is aware of your intrusion and will actively interfere with your activities while directing IC and/or security hackers your way, and may take even more drastic measures to block your hacking attempts.

HACKING AND ACCOUNTS

Hackers can gain passcodes to accounts in many ways: stealing them, shoulder-surfing, or sniffing traffic online (see p. 224). Hackers can copy passkeys if they have the actual passkey or its schematics. Counterfeiting a key requires that the encryption be broken first. It then takes a Hardware + Logic Extended Test (10, 1 day). Hackers can also manipulate accounts on nodes they have compromised with an Edit action (p. 218).

Note that many systems periodically require their users to change account passcodes for security reasons, so passcodes rarely last forever. Likewise, any accounts linked to security anomalies will typically be locked out until an investigation determines they are safe.

If a hacker wants to get into a node but has not acquired a passcode, then he must break in.

BREAKING IN

There are two methods a hacker may employ to break in: on-the-fly hacking and probing for weaknesses.

Hacking on the Fly

On the streets or during a run, you will undoubtedly encounter situations where you need to hack into something without any sort of preparation. In circumstances like this, you pull out all of your hacker tricks and tools and do your best to quickly find an exploit that will get you in without alerting the node's security—or you simply may not care if you trigger an alarm. Hacking on the fly tends to be a brute-force affair—success is more important than subtlety or finesse.

To hack on the fly, you spend a Complex Action and make a Hacking + Exploit (Firewall, 1 Initiative Pass) Extended Test. This will get you personal account access; if you want security-level access, increase the threshold by +3, or +6 for admin access. If you beat the threshold, you have bypassed the security and now have access to the node.

Each time you make a test to hack in, however, the target node also gets to make a free Analyze + Firewall (Stealth) Extended Test. If the node detects you—whether you hack in or not—an alert is triggered (see *Intruder Alerts,* p. 222).

Probing the Target

If you have the time to properly case your target, your hacking attempt is more likely to be successful and unnoticed. Using this method, you discreetly probe your target over an extended timeframe, identifying system flaws that can be exploited for access.

Probing is handled as an Extended Hacking + Exploit Test with a threshold equal to the target's System + Firewall. The interval is 1 hour if done in VR, 1 day if done by AR. This will get you personal account access; if you want security-level access, increase the threshold by +3, or +6 for admin access. Once you reach the threshold, you have found a crack in the system's defenses that you can exploit to gain access. Using this exploit takes a Complex Action, but automatically succeeds. At the gamemaster's discretion, such exploits may even work repeatedly (serving as an effective back door into the system), unless the node is somehow alerted to the weakness. Such back doors may also not last forever, as security upgrades or regular system audits may close off that access route.

Similar to hacking on the fly, the target node gets one free Analyze + Firewall Test when you make the actual intrusion. The threshold for this test equals your full Stealth program rating. If the node detects you, an alert is triggered (see *Intruder Alerts,* p. 222).

Glitches: If you glitch while conducting your probing, the target node is alerted to your reconnaissance attempts. At the gamemaster's discretion, you may need to start over, the node may be prepared for your exploit attempt (receiving a bonus