Voice recognition systems require a vocal response from an approved user's voice, usually within a certain amount of time. If the response is not given within the time limit, or someone not approved answers, the system sounds an alarm. Characters can only defeat voice recognition systems by "speaking" with the voice of an approved user—by using a recording, some other simulation, or the real voice. Voice modulator cyberware (see p. 332) can also be used. An Opposed Test must be made between the voice recognition system and the equipment used to bypass it; whichever generates more hits, wins.

Breath, cellular and DNA scanners collect a sample of the user's cells, either off the finger/palm, via hair suction, through exhaled particles, or something similar, and analyze the genetic material. In order to fool such a system, you need a sample of the correct genetic material, preserved in a specially formulated enzyme bath. The enzyme bath can be synthesized in a chemistry shop with a Chemistry + Logic (5, 1 hour) Extended Test.

Facial recognition scanners use imaging lasers, thermographic, and/or ultrasonic waves to map a person's face. These are one of the least intrusive, but also least accurate, of biometric recognition systems. Facial recognition systems are useful not just for letting authorized people in, but also for identifying unwanted people and keeping them out. Prosthetic makeup and biosculpting can be used with varying degrees of effectiveness against facial recognition; make an Opposed Test pitting Disguise + Intuition against the Device rating. Apply a +2 modifier to the character if the system is picking the disguised character out of a crowd.

Automated Systems

Automated security systems provide an immediate, automatic response to tripped alarms.

Automated gun systems are simply weapon-mounted drones placed in fixed locations (usually with a 180 degree firing arc) or on slide-mounted track systems. These systems are typically loaded with basic sensors and Targeting autosofts and follow all the standard rules for drones (see p. 238).

Containment systems entail a kind of trap mechanism: when an alarm is triggered, shutters drop down over windows, doors shut and lock, and sliding walls or gates may be activated. They may also include laser or monowire mazes and radio jamming. The objective is to detain intruders within a confined area, after which they may either be removed or "neutralized."

Gas delivery systems can be insidious, dispersing gas in a potentially undetectable manner. Dispersal systems can fill an area of 30 cubic meters in one Combat Turn. The gamemaster determines how far and how quickly a gas spreads. The gamemaster may secretly conduct Perception Tests to see if any characters detect the gas, basing the threshold on the noticeability of the gas used (many gases are colorless and odorless). Characters equipped with a olfactory scanner (see p. 326) may be alerted by their gear. See p. 244 for details on various gases and how they will affect characters.

Marking systems are designed to tag intruders with a discreet marking so that they can be later identified if captured. Marking methods include ultraviolet dye, RFID tags, DNA-encoded material, or even nanite tags. The markers are typically sprayed unobtrusively over exitways and other traffic areas.

MAGICAL SECURITY

There are a number of methods used to keep astral intruders out, the most common of which are bound patrolling spirits and astral barriers such as wards (see p. 185). Various dual-natured paranormal critters are often used as watch animals, as they can detect and attack astral as well as mundane targets. Respectable security companies train their guards to detect the "shivers" that mundanes sometimes feel when an astral form passes through them (see p. 183).

Some sites with security magicians on hand utilize the Mage Sight fiberoptic system (see p. 326).

Biofiber

Biofiber is a form of bio-engineered plant life similar to wood, grown in large, flat sheets. Biofiber is naturally dual natured, existing on the astral and physical planes simultaneously. So long as the biofiber is kept alive (using complex nutrients), it functions as a barrier against astral forms, just like a physical wall. The biofiber has a Force rating like any other astral barrier and functions in the same manner (see p. 185). Biofiber sheets are placed inside the walls of high-security areas, provided with nutrients and carefully monitored. Destroying the astral barrier kills the biofiber. Biofiber is notoriously sensitive and difficult to maintain. It is available in a maximum Force Rating of 10.

MATRIX SECURITY

Most businesses utilize wireless networks for convenience. To protect these networks from intrusion, however, they are often encrypted and operated in hidden mode, set to only interact with specified devices. Others operate with an extremely low Signal rating, so that you must be well within corporate grounds to access the network. High-security systems will avoid wireless altogether, sticking to an internal wired network that is either completely isolated from the Matrix, or linked via secure gateway networks, perhaps through carefully timed and temporary connections. In order to access such systems, a hacker must usually break in and acquire a physical jackpoint connection. Individual systems will be guarded by IC and security hackers, as well as other measures like data bombs and encrypted files (see p. 222).

Wi-Fi Negation

Wi-fi-inhibiting paint and wallpaper are commonly used to prevent an internal wireless network from leaking outside of a building—and to prevent intruders from extending their own networks inside. Wi-fi negation schemes are treated like jammers (p. 321); any Signal rating less than the negating system's rating cannot extend past the boundary.

Wi-Fi Detection

Many security networks—especially those monitored by spiders—automatically scan local wireless networks within range for signs of unusual activity. These networks will take note of new networks, perhaps even intercepting the signal to monitor or sniff out illicit activity. Security may even triangulate a network using multiple signals to determine of the network