Dirty Tech: Homemade Surveillance Gear

Regardless of its Legality Class, surveillance gear is difficult to acquire "no strings attached." Even in low-Control Rating areas, simply buying a bug or a wiretap from a novelty "spy shop" can attract unwanted attention. A credit card leaves a paper trail – and while you can always pay cash, anyone who sells security cameras will almost certainly have video of *you* making the purchase!

Luckily, such equipment isn't difficult to build. The parts are common enough that purchasing them attracts little attention, and you might even be able to scavenge what you need from electronics purchased at a garage sale or dug out of the trash – a great use for Scrounging! Most audio and video bugs require about half a day's work, $10 to $20 in materials, and an Electronics Repair (Surveillance) roll. Tiny projects are hard to pull off with a soldering gun, though. For any device smaller than a matchbox (SM -9), apply SM+9 as a penalty to skill; e.g., a 1/2" audio bug (SM -13) gives -4.

Subminiature Video Bug (TL8). The smallest video bugs are the size of a multivitamin capsule (SM -13); in fact, they're used to diagnose intestinal problems when an endoscope would be too invasive. Transmitter range is less than 500 yards. The special internal battery lasts for 48 hours. $1,500, neg. LC3.

Video Bug (TL8). An over-the-counter "spy shop" video bug is still a capable surveillance device. About the size of matchbox (SM -9), it can transmit a high-quality video signal up to two miles away. $250, neg., T/week. LC4.

Tracking Devices (TL7)

Tracking devices range from the benign – like the personal rescue beacon (p. 59) – to the more sinister "tracking bugs" used for surveillance. All communicate via radio and are subject to that medium's inherent limitations (see *Radio,* pp. 37-40).

Radio Beacon (TL7)

This is the classic Hollywood "tracking beacon" – a radio transmitter designed to be attached to a vehicle, hidden in a briefcase, etc. Its signal is detected using a radio direction finder (pp. 38-39). Anyone scanning for bugs has +4 to find this "noisy" device. Each tracker has a special coded signal that allows those who planted it to recognize it easily. Range is 25 miles.

Radio Beacon (TL7). $300, 0.5 lb., S/month. LC4.

Radio Beacon (TL8). $300, 0.25 lb., XS/month. LC4.

Cell Phone (TL8)

Cell phones (p. 39) broadcast a constant identification signal while turned on, even when not making calls. This is how the cellular network "knows" where to route incoming calls. Those with access to the network – e.g., government agents with a subpoena – can fix a cell phone's location to within half a dozen blocks in an urban area or a few miles in a rural setting.

Cellular Locator Beacons (TL8)

A cellular locator beacon is a GPS receiver (p. 53) that communicates its current position – accurate to within a few feet – over a cellular telephone network. A service ($50/month) is available that lets anyone with an Internet connection and the correct password track the beacon in real time. The locator may be set to transmit a record of its position history at regular intervals and then switch off its transmitter. While this prevents tracking in real time, it saves power and reduces the chance of detection. Multiply battery life by 10 for hourly updates, 100 for daily updates.

Cellular Beacon (TL8). This device can run off its onboard battery pack or be connected to a vehicle's power supply for indefinite operation. It must be in reach of a cellular network to relay its position, and is susceptible to jamming. *Triple* cost for a version that uses satellite phone (pp. 39-40) technology, which can be tracked anywhere in the world. $1,500, 1 lb., S/week. LC4.

Personal Cellular Beacon (TL8). This is a smaller unit built into a wristwatch, bracelet, shackle, etc. $400, 0.1 lb., T/month. LC4.

Encryption

Encryption is a body of techniques for concealing a message's meaning from anyone but the intended recipients. It's crucial at TL6-8 owing to the prevalence of easily intercepted telecomm technologies. The wars of the first half of the 20th century drove this point home, with encryption (and its defeat) influencing several prominent successes and failures.

Encryption takes two basic forms:

- A *code* is a series of prearranged secret meanings; e.g., "One of by land, two if by sea."
- A *cipher* is a method of transforming data – whether via a simple substitution (e.g., Morse code) or a mathematical algorithm. The strongest ciphers disguise the signal as seemingly random gibberish. A recipient who has the key can "decrypt" the message and extract its information.

Code-Breaking (TL5)

In 1929, Henry L. Stimson – U.S. Secretary of State at the time – quipped, "Gentlemen do not read each other's mail," and closed the U.S. State Department's cryptographic unit (the Black Chamber). Meanwhile, unbeknownst to Stimson, the U.S. Navy and Army were intercepting Japanese traffic. Overseas, Britain and Poland were working like mad to defeat the Enigma machine (see *Cipher Machine,* p. 211).

To break a simple, ad-libbed code or cipher, *win* a Quick Contest of IQ-5 with its creator. Either party may substitute the Cryptography skill (p. B186). Beating the systems under *Encryption Devices* (p. 211) and *Encryption Standards* (p. 211) *requires* Cryptography, however.