

The list of eighteen state of the art equipments used for advanced spying

1. Binoculars

Visually observed speech can be read using the Lip Reading skill. Spotting observing binoculars requires a Vision roll (often also aided by binoculars) with the normal vision modifiers for small size, range, bad visibility, darkness and concealment (e.g. the binocular can be hidden behind a tinted window, mirror, curtain or camouflage veil). But the unwanted observer is also hindered by most of the same vision modifiers. The recent anti-sniper laser systems are able to detect optical systems (e.g. telescopic rifle sights or binoculars) by analyzing their laser reflection. If such a system is available detection requires one successful Electronics Operation (Sensors) roll for every binocular.

2. Bugs

Small concealable, voice-activated microphones, sometimes with digital recording and burst radio transmission, or with immediate transmission are called "bugs". A good state-of-the-art bug detector and a successful roll against SIGINT Collection/Jamming or Electronic Operation (Sensors) will find a bug with a slow and thorough examination of the area.

3. Camcorder

Electronic imaging and recording devices have uses and weaknesses similar to binoculars. On the down side may be the time lag when the recorded information is analyzed some time after recording. This can be avoided by instantly transmitting the signal via radio, laser or cable. The last methods are preferable because radio transmissions can be detected passively. On the upside of camcorders are the much reduced size compared to an observer with binoculars and the possibility to install the camcorder at hard-to-reach hidden locations. To spot observing camcorders requires a Vision roll (often also aided by binoculars) with the normal vision modifiers for small size, range, bad visibility, darkness and concealment (e.g. the camcorder can be hidden behind a tinted window, mirror, curtain or camouflage veil). But the camcorder is also hindered by most of the same vision modifiers (darkness can be canceled by electronic light intensification and infrared imaging). The recent anti-sniper laser systems are able to detect optical systems (e.g. telescopic rifle sights, camcorders or binoculars) by analyzing their laser reflection. If such a system is available detection requires one successful Electronics Operation (Sensors) roll for every camcorder.

4. Computer Taps

If an interested party had access to your computer it might have "upgraded" it with unwanted features. Think about that. The computer can be modified to act as a camera, microphone or it can collect information stored on its drives or transmitted through the network it is connected to (not necessarily information intended for this particular

computer within the network). Whatever the information, it can be stored (e.g. in a dedicated "extra-memory"), compressed, encrypted and transmitted by various means. Useful channels include telecommunication lines, electric power lines, data network lines, radio broadcast, printed documents (e.g. by slightly changing the letters in a text) and publicly displayed information (e.g. as in an airport display, or a customer information terminal). To detect unwanted data processing in a computer is very hard (Electronic Operation [Computers] -8). To physically detect any unusual modifications is sometimes impossible since with certain systems no physical modifications are needed. Most "multimedia" computers already have anything onboard that is required to turn them into instruments of surveillance. To detect unusual data transmissions requires TEMPEST equipment and a roll against Electronics Operations (Sensors).

5. Eavesdropping

The old-fashioned but still working way to gather intelligence. No electronic sensors can detect compromised loyalties. Possibly unreliable persons should not be allowed unobserved near sensitive information (e.g. for cleaning or maintenance). And carriers of said information should never discuss them outside of secured areas (e.g. in the cantina).

6. Electric Power Line Bugs

A bug does not have to use radio for transmission. It can use the normal electric power distribution network to send information "backwards" to outside receivers. The bug itself can be hidden in plain power lines, sockets or small transformers (e.g. for connecting laptops or battery chargers to power outlets). To detect an electric power line bug requires appropriate equipment and a roll against Electronics Operations (Sensors).

7. Electromagnetic Induction

Without going too deep into physics it is safe to assume that each two electrically conducting wires that run parallel and more or less close influence each other by electromagnetic induction. This effect is well known from older analog telephone lines as the faint voices sometimes audible in the background. Most communication cables are bundled in cable tubes, sometimes parallel to power lines. Depending on the used cable type, the distance, the length of the parallel section, and the type of signal transmitted through the first cable, it is often possible to detect, filter and enhance the induced signal from the second cable. If, for instance, digital information from a computer network cable is induced into an analog telephone line or a simple power cable, it will not be immediately obvious as a security breach. If a cable leaves a secure zone after running in parallel for at least two yards to a cable transmitting sensitive information this information may be extracted with specialized equipment not larger than a laptop computer. Use Electronic Operations (Sensors) skill to operate said equipment. And aside from physically stumbling over someone operating this equipment and recognizing what he is up to, there is no way to detect this kind of surveillance.

8. Electronic or Acoustic Stethoscopes

Using an electronic or acoustic stethoscope is technically augmented eavesdropping. Like next to all other electronic equipment, electronic stethoscopes get smaller, better and less expensive all the time. The sensor (microphone) of such a device might look like any plane item (e.g. a picture or sign). Linking a stethoscope to a bug lets it function through at least one yard of solid structure. If this structure is shielding electromagnetic waves this makes it considerably harder to detect the electronic stethoscope (and bug); all detection rolls are at -1 to -4 (GMs decision). It is impossible to detect the use of an acoustic stethoscope other than finding it with a physical search.

9. Fiber-Optic Scopes

These can see into a room from any very small spot. They have similar uses like binoculars and camcorders. The optic cable transmits the picture either to an outside monitor or to a recorder. Of course, the signal can be transformed into radio signals or beamed laser communication to bypass outside security. Speech can be read by Lip Reading skill or a laser microphone can be combined with the fiber-optic scope. Other visual information like computer screens, hardcopies, or the filmed typing on a keyboard may also be of use. With the creative use of reflective surfaces, zoom and image enhancing software amazing results can be achieved. To detect fiber-optic scopes requires a Vision roll at -12 during a very thorough examination of the area. This is complicated by the fact that fiber-optic scopes are mostly installed at hard-to-reach and/or hidden locations, like in ceiling structures or behind mirrors.

The recent anti-sniper laser systems are able to detect optical systems (e.g. telescopic rifle sights, camcorders, fiber-optic scopes or binoculars) by analyzing their laser reflection. If such a system is available detection requires one successful Electronics Operation (Sensors) roll for every scope.

10. High-Frequency Modulation

Since the early fifties the worlds secret intelligence organizations use high-frequency modulation for surveillance. This technique requires no inside power source and is very hard to detect because it lacks any microphones or circuits. An outside HF-transmitter targets a strategically placed small device, that modulates this wave by passively vibrating the reflecting antenna cylinder in correspondence to surrounding sound waves. To detect active HF modulation requires a bug detector and a roll against Electronic Operations (Sensors). To detect the small reflector device when it is not reflecting requires the same roll at -4. Note that the active part is always the outside HF-transmitter, not the reflector device.

11. Laser Microphones

By picking up invisible laser reflections from vibrating surfaces like windows these devices can read sound over long distances. Detecting a laser microphone is possible with a laser detector and roll at +2 against Electronic Operation (Sensors) skill, but the

detector has to be directly in the path of the laser beam or it needs a line of sight to the reflecting surface.

12. Long-Range Microphones

By collecting and concentrating sound with parabolic dishes these microphones can produce useable results at over 2,000+ yards. Modern ones use electronic filtering programs to eliminate background noise. A long-range microphone may be spotted with the normal vision modifiers for small size, range, bad visibility, darkness and concealment (e.g. the microphone can be hidden behind a curtain or camouflage veil).

13. Microphones

Any microphone or speaker already in a room can be modified to transmit sound through existing wires or a dedicated very thin wire to an outside recorder or listener. Or a very small microphone is placed in the room exclusively for that purpose. Other good places for microphones are ventilation ducts, heating or water tubes, at a position not necessarily close to the target room because these ducts and tubes carry sound very well over long distances. A good state-of-the-art bug detector and a successful roll against Electronic Operation (Sensors) skill will find them with a slow and thorough examination of the area where the bug is placed.

14. Phone Taps

Even an inactive phone, if modified to do so, can transmit sound using the standard phone cable. It draws power from the same cable and can run indefinitely that way. Modern electronic phones can contain built-in taps that are only detectable with a complete tool set or bug detector and a roll versus Electronic Operation (Communications) or Electronic Operations (Sensors). More simple taps may be detected by visual inspection of the telephones inside hardware and a roll against Electronic Operation (Communications) -4. A phone tap does not need to be inside the phone itself, but can also sit in the phone socket in the wall or anywhere along the line.

15. Revealing Acoustic Emissions

Recording and processing acoustic emissions other than plain speech is a combination technique. Some printers make distinctive (ultrasound) noises during printing. These are directly correspondent to the information that is printed. If recorded, this printing noise can be used to reconstruct the printed information, using computer programs. Other simple examples of revealing noises are the dialing sounds of telephones, especially if using loudspeakers. Anyone listening can reconstruct the dialed numbers. Listening to acoustic emissions is done by one of the above mentioned ways: by bug; by computer tap; by stethoscope; by HF modulation; by laser microphone; by microphone; or by phone tap.

16. Revealing Electromagnetic Emissions

TEMPEST gear (short for Transient ElectroMagnetic Pulse Emission Scanning Technology) reads the radio frequency emissions of computer monitors or printers and translates them back into readable information. TEMPEST gear has grown smaller, better and cheaper in the last years. Portable equipment, not larger than a laptop computer plus hand-held parabolic antenna is already available (GURPS Ultra-Tech 2 rates this as TL8; yes, its early TL 8). The only protection against TEMPEST gear is a closed faraday cage and/or electronic shielding of all emitting equipment. But since any conductor functions as an antenna, radio frequency emissions may bypass a faraday cage and electronic shielding simply by "riding" power lines or communication lines. There is no way to detect TEMPEST surveillance. The best defense besides faraday cages and electronic shielding is distance. Keep any potential scanners as far away from your computers and printers as possible.

17. TV-Receiver Bugs

Any receiver antenna can be used to transmit as well. A television receiver antenna is a nice way to send a very long ranged signal, compared to the miniature antennas of most other radio emitting bugs. The television set also has a ready power input and a speaker or speaker system that can be used as a microphone with little modification. Even placing a camera is no big deal inside some television sets. Detection is complicated by the fact that microphone and antenna are separated and that TV antennas are frequently at hard to reach outside positions. But a good state-of-the-art bug detector and a successful roll against Electronic Operation (Sensors) -2 will find a TV-receiver bug

18. Cellular Phones

A cellular phone can compromise acoustic information even if turned off. Depending on model some cellular phones can be silently activated from the outside. This allows to initiate transmission of everything audible within the range of the phone's microphone. The only fairly secure way to prevent this is to remove the batteries from the phone. This will not work if the phone has been modified (e.g. upgraded with a second hidden power source) to prevent this. Any transmitting phone can be detected with suitable equipment and a successful SIGINT Collection/Jamming, Electronic Operations [Sensors] or Electronics Operation [Communications] roll. .