Григор'єва А., курсант ННІ №1
Національної академії внутрішніх справ
Консультант з мови: **Марченко І.В.**

USING WIRETAP IN COMBATING CRIME

1.What is wiretapping?

Wiretapping is the surreptitious electronic monitoring of telephone, telegraph, cellular, fax or Internet-based communications.

Wiretapping is achieved either through the placement of a monitoring device informally known as a bug on the wire in question or through built-in mechanisms in other communication technologies. Enforcement officials may tap into either for live monitoring or recording.

The history of wiretapping:

Wiretapping laws have always had difficulty in balancing privacy rights of individuals with the concerns of state and law enforcement. While wiretapping has existed since the days of the telegraph, the first recorded wiretapping by law enforcement was in the 1890s in New York City. In the 1910s, the New York State Department found that police had wiretapped entire hotels without warrant. The department claimed it did not violate Fourth Amendment rights, on the grounds that the amendment only covers tangible communications, such as mail, and that it only breached those rights where placing of taps involved trespassing. (That restriction was no block to enforcement, as officials could tap a telephone company's switching station.)

Modern-day wiretapping:

The argument that new technologies are not covered by the law is often used to justify increased monitoring of private citizens. The Electronic Communications Privacy Act (ECPA), despite its name, loosened the requirements for non-voice based communications, and the Communications Assistance for Law Enforcement Act (CALEA) of 1994 allowed law enforcement to fine telcos $10,000 a day if the company's networks are not built with wiretapping capabilities.

Concerns have been raised by the National Security Agency's (NSA) monitoring of private citizen communications since it was revealed that they have been wiretapping on a broad scale without even a stated justification. Concerns are often dismissed because only metadata is collected, rather than the content of messages, but even that data can be extremely revealing. An increasing number of technological hardware and software systems are designed or adapted to include wiretapping capabilities, including IPv6, which is expected to expand the number of Internet-connected devices exponentially.

1. Types of wiretaps

If you are concerned about covert eavesdropping then it may be wise to contact Granite Island Group, or another TSCM firm and immediately schedule a "Bug Sweep" or TSCM inspection. However, do not call from a suspect telephone, and understand that it is critical that you get some out to your location as quietly, and as quickly as possible.

Bugging (Everybody's Favorite Subject)

A "Bug" is a device that is placed in an area, which then intercepts communications and transmits or conducts them out of that area to a listening post. The eavesdropper can be just a few feet away from the victim, hundreds of feet, or even miles away depending on the kind of bug used.

There are five primary categories of "Bugs":

- Acoustic
- Ultrasonic
- RF (Radio Frequency)
- Optical
- Hybrid

1. An Acoustic Bug is the placing of a water glass, stethoscope, or rubber tube into an area and directly intercepting the communication with the naked ear (without the use of electronics). This also applies to sections of an area where sound is leaking though soft spots around windows, structural defects, ventilation structures, poorly installed power outlets, and so on.

2. An Ultrasonic or VLF Bug is a technique use to convert the sound into an audio signal above the range of human hearing; the ultrasonic signal is then intercepted nearby and converted back to audio. In this case audio pressure waves are used instead of creating a radio signal.

3. An RF (or Radio Frequency) Bug is the most well known type of bugging device. A radio transmitter is placed in an area or in a device. This is your classic martini olive bug and "spy shop" store device. These are extremely easy to detect, cheap, disposable, but difficult to trace back to the person who

actually planted it. A properly equipped TSCM specialist can actually detect this kind of device at a significant distance, but it does require some time to properly accomplish this task. Keep in mind that any legitimate bug sweep takes hours, or even days, but not minutes).

4. An Optical Bug is a bugging device that converts sound (or data) into an optical pulse or beam of light. It is rarely used, expensive, but easy to detect. A good example of this would be active or passive laser listening device.

Any of the above techniques and devices can be combined to make a Hybrid eavesdropping device.

Wiretapping

Wiretapping is the preferred method of obtaining intelligence (for quality reasons), it involves tying into a wire or other conductor that is used for communications. This wire can be a telephone line, a PBX cable, a local area network, a CCTV video system, an alarm system, or any other communications medium. The goal in a wiretapping is to secure high quality information, and to minimize the possibility of the eavesdropping being detected (remember radiated signals are easy to detect). Look inside of your "electrical or phone closet" at your office to see how easy it would be to plant a bug!

Wiretaps are broken into four primary categories:

- Hardwired
- Soft
- Record
- Transmit

A Hardwired Wiretap, is when physical access is gained to a section of wire that the signal (i.e.: telephone line) travels on. A second set of wires is attached (normally through the use of an isolation or slave device), the signal is then bridged back to a secure location. This type of wiretap when discovered is fairly easy to trace back to the listening post. This type of wiretap is very popular with the police, but is usually outside the scope of most eavesdroppers. If the eavesdropper is using a "slave" or similar isolation device on a telephone the tap will be virtually impossible for anybody except a highly trained or properly equipped "bug sweep" professional to find (and there only around a dozen of these in the US).

A Soft Wiretap, is a modification to the software used to run the phone system. This can be done at the telephone company, or in the case of a business, the PBX. A soft wiretap is a preferred method to tap a phone, easy to catch on a PBX, but tougher to find in the phone company's system. It is sometimes called a REMOBS (REMote OBServation), DATU, ESS, or translation tap. This type of tap is very popular with large law enforcement agencies, intelligence agencies, larger corporations, and with hackers who find it quite simple to gain access via maintenance software. This type of tap is actually very simple to find, but does require completely un-restricted access to the inner workings on the phone company's computers (which is very tough to obtain).

A Recording Wiretap, is nothing more than a tape recorder wired into the phone line, very easy to find on a TSCM inspection. Similar to a hardwired wiretap, but the tapes must be changed on a regular basis. This is very, very popular with amateur spies, and private investigators, but they are very dangerous to use, and many eavesdroppers have been caught red-handed when they showed up to service their illicit recorder. Digital recorders are replacing tapes, but as with the tape recorder, someone has to retrieve the data.

A Transmit Wiretap, is an RF transmitter (or "Bug") connected to a wire (often containing a microphone itself). This type of tap is very popular, however; the RF energy it produces radically increases the chance that it will be detected by a competent "Bug Sweeping" specialist (known in the business as a "TSCM Specialist" or Practitioner).

Wiretaps are extremely difficult to detect (if properly installed), require a very high level of technical expertise, and a great deal of equipment to locate. It is virtually impossible to detect most wiretaps with any spy shop toy, bug detectors, and other such gizmo's. Instead the TSCM specialist has to use hundreds, and often thousands of pounds of highly sophisticated laboratory grade instruments, and perform hundreds of highly sensitive measurements.

Список використаних джерел

1. Granite Island Group. Types of Wiretaps, Bugs and Methods – [Електронний ресурс]. – Режим доступу : http://www.tscm.com

2. Tom Harris. How Wiretapping Works – 2017. – [Електронний ресурс]. – Режим доступу: https://people.howstuffworks.com

3. Susan Landau. The risks of new wiretapping technologies – 2014. – [Електронний ресурс]. – Режим доступу: http://whatis.techtarget.com