

Seizing the Signals

Electromagnetic signals

- | Waves propagating through some medium
 - Air, water, copper wires, fiber optics, etc.
 - Frequencies (Hz): wave cycles per second
 - Bandwidth: difference between the lowest and highest frequencies
- | Electricity, radio spectrum, infrared, (visible) light, x-ray, etc.
- | Advantages/disadvantages
 - Low frequency: hard to jam
 - High frequency: larger bandwidth

Signal Intelligence (SIGINT)

Operations that involves

- interception
 - analysis
- of signals across electromagnetic spectrum.

Intelligence report, criminal investigations, employee monitoring

Digital signal processing

- Communication intelligence (COMINT)
- Electronic intelligence (ELINT)
- Imagery intelligence (IMINT)

Eavesdropping



Passive Attack

- | Access to confidential data and traffic pattern
- | Privacy rights
- | U.S. federal wiretap law
 - Illegal for an individual to eavesdrop intentionally on wire, oral or electronic communications
 - Home usage? Bug your phone? Hidden recorders?
 - Company monitoring? Computer vs. telephone?
- | Eavesdropping device: manufacture, sale, possess, advertise
 - Legal/illegal?
 - The Spy Factory

CSCE 727 - Farkas

5

Telephone Wiretap

- | Physical access
- | Gain:
 - Sensitive data (e.g., organizational secret, private information, etc.)
 - Disallowed information (e.g., law enforcement communications)
- | Federal wiretap restrictions
- | Individuals and organized crime wiretap
- | Cellular scanners
 - Cellular phone calls
 - 1994 – illegal in USA (import, manufacture, sale)
 - Homemade scanners?
- | Pager Intercept

CSCE 727 - Farkas

6

Law Enforcement Wiretap

- | Federal Government and state government (37 states): authorized to intercept wire and electronic communications
 - Court order
 - Probable cause of criminal activity
 - Only relevant information
- | Phone and room bugs, computer monitoring
- | Organized crime monitoring (drug trafficking, terrorist activities, etc.)
- | Legislations:
 - 1986: Electronic Communications Privacy Act, Title III.
 - 1978: Foreign Intelligence Surveillance Act
- | Encryption

Foreign Intelligence Intercepts

- | National Security Agency
 - Monitor everything (microwave, satellite, phone, etc.)
 - Information about allies and enemies
 - Disallowed to spy on U.S. citizens
- | NSA's "ears" cover the globe
 - Political and military intelligence (nuclear weapons, chemical warfare, etc.)
 - Government trade secrets and economical information
 - Terrorist activities

Foreign Intelligence

- | Five-nation alliance (1948)
 - U.S.A., United Kingdom, Australia, Canada, New Zealand
 - Five spheres of influence of the Earth
 - Each country to monitor a sphere
 - Concerns:
 - | Privacy violations
 - | Corporate information
- | Other nations intelligence: Russia, Japan, France, etc.

Message Deciphers

- | Available encryption technology
- | Cryptanalysis
 - Technology
 - Brute force attack
- | Other means
 - Spy, social engineering, eavesdropping, keystroke monitoring, hacking, etc.
- | Release information → give our capabilities
 - National defense, tactical, ethical, etc.?