Electronic and Information Warfare

Security Engineering Chapter 19

Presented by Jad Silbak.
Seminar Instructor: Professor Orr Dunkelman.

Electronic and Information Warfare

- To understand Information Warfare (i-war), let us first define and understand Electronic Warfare (i-war).

- Why should we care?
  - If you are interested in computer security, e-war may have great lessons for you.
  - Private companies use some of electronic warfare tools.

What is E-war

- What is electronic warfare?
- What do we value most in e-war?

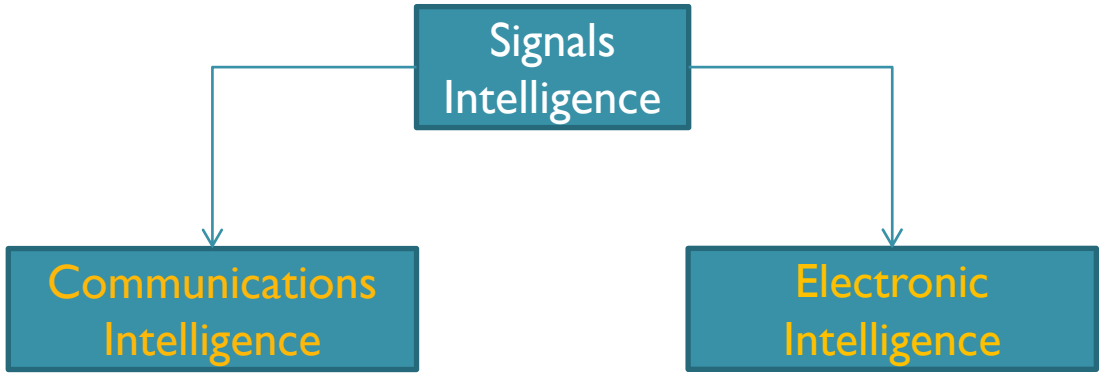
Computer security	Electronic warfare
Confidentiality	Denial of Service (jamming, physical attack)
Integrity	Deception
Availability	Exploitation (eavesdropping)

Importance

Control of the electromagnetic spectrum

- Electronic attack
  - Jamming enemy communications.
  - Disrupting enemy equipment using high-power microwaves.
- Electronic protection
  - Designing systems resistant to jamming.
  - Hardening equipment to resist high-power microwave attack.
  - Destruction of enemy jammers using anti-radiation missiles.
- Electronic support
  - Supplies the necessary intelligence and threat recognition, to allow effective attack and protection.

Electronic support



Comint	Elint
We are interested in the communications among people.	Non-communications signals intelligence, such as radars.
Who is transmitting? Where they are located? The time and duration of transmission?	Elinet can be used to detect ships and aircraft by their radar and other electromagnetic radiation, missile firing signals
If the transmission is encrypted or not?	Identify-Friend-or-Foe

https://en.wikipedia.org/wiki/Signals_intelligence

Communications Systems

- Military communications were dominated by physical dispatch until about 1860.
  - Marathon story of Philippides.

- About 156 years into the future things are different.

https://en.wikipedia.org/wiki/Pheidippides http://www.telcomhistory.org/timeline.shtml

Communications Systems

- Situational awareness and the means to direct forces, are critical in warfare.
- Possible threats
  - Communication between the army and the political leadership can be compromised, or the link might be disrupted.
  - For agents in the field location security is important.
  - Control and telemetry communications, such as signals sent from an aircraft to a missile it has just launched, must be protected against jamming and modification.

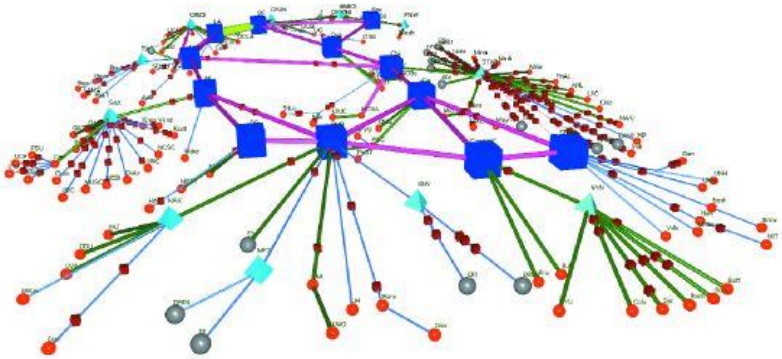
Communications Systems

- Effective defense needs:
  - Content secrecy
  - Authenticity
  - Resistance to traffic analysis and radio direction finding.
  - Resistance to various kinds of jamming.

Signals Intelligence Techniques

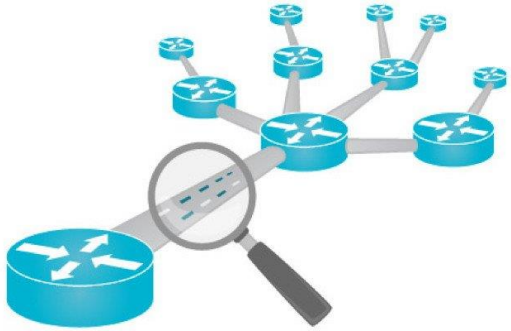
- Before communications can be attacked, the enemy's network must be mapped.

  - Radio Direction Finding (RDF)
    - Triangulating the signal of interest.
    - Time difference of arrival.
  - Traffic analysis.
    - Snowball search.
    - De-anonymization.



Traffic Analysis

- Looking at the number of messages by source and destination, can give very valuable information:
  - Imminent attacks
  - Unit movements.
- Traffic analysis is even more interesting when sifting through traffic on public networks.



Traffic Analysis

- De-anonymization
  - More than 81% of Tor clients can be identified with traffic analysis attack.
  - The NSA can do more .. way more.

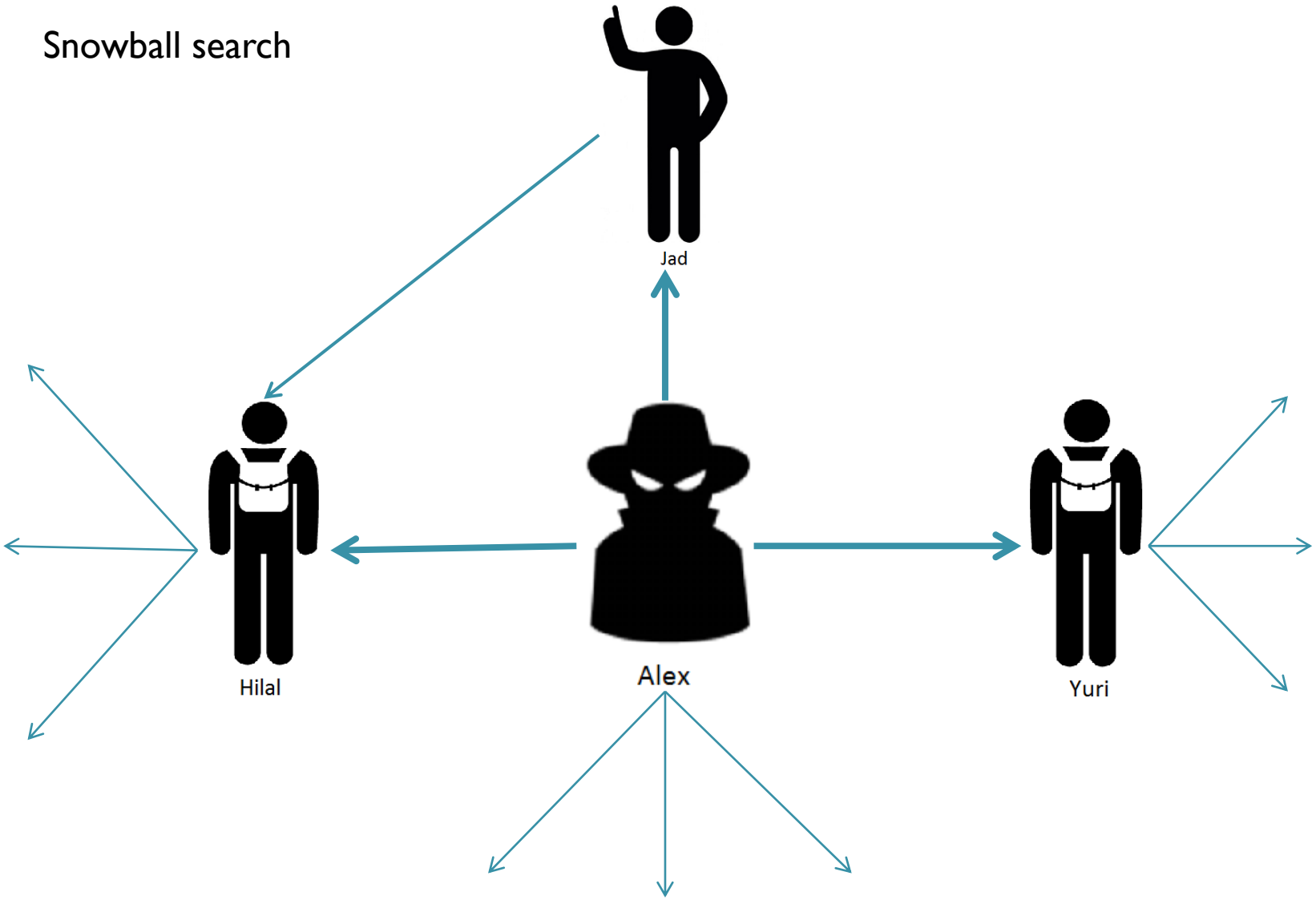
https://thestack.com/security/2014/11/14/81-of-tor-users-can-be-de-anonymised-by-analysing-router-information-research-indicates/

Traffic Analysis

- Traffic analysis can used to identify a malicious or suspicious packets within the traffic.

- Snowball search.

Snowball search



Traffic Analysis

- Content generally has to be selected in real time.
  - Not even the NSA can afford to store all the data on the Internet and the phone networks.
  - The most difficult and expensive part is traffic selection rather than collection.

- Is encryption the solution?

Cryptography VS Traffic Analysis

- Cryptography can make communications more vulnerable.
  - If you just encipher all the traffic you consider to be important, you have thereby marked it for collection by the enemy.
  - And even if your cryptosecurity were perfect, you've just helped the enemy map your network, which means he can collect all the unencrypted traffic that you share with third parties.

Cryptography VS Traffic Analysis

- Possible solution
  - Every one should encrypt all their traffic, thus hiding traffic could be much easier,
  - masking the channel by sending dummy traffic.
- Intelligence agencies have been trying to prevent the widespread use of cryptography, even if it's freely available to individuals.

https://en.wikipedia.org/wiki/Export_of_cryptography_from_the_United_States

FBI–Apple encryption dispute

- FBI announced that it was unable to unlock the county-owned phone it recovered in the 2015 San Bernardino attack.
- Going dark.

https://www.youtube.com/watch?v=zsjZ2r9Ygzw

https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute#FBI_withdrawal_of_request

Attack on Communications Systems

- In tactical situations, the goal is often to detect and destroy nodes, or to jam the traffic.
- Jamming can involve not just noise insertion but active deception.
  - In World War 2, the Allies used German speakers as bogus controllers to send German night-fighters confusing instructions.

Attack on Communications Systems

- Generally requires a combination of techniques .
- Owen Lewis sums it up Soviet doctrine, an attack on a military communications infrastructure would involve
  - destroying one third of it physically,
  - denying effective use of a second third through techniques such as jamming, trojans or deception,
  - and then allowing the adversary to disable the remaining third by attempting to pass all his traffic over a third of his installed capacity.

Protection Techniques for Communications Systems

- What do we need for an effective Protection of the communication systems?
  - Authenticity and confidentiality,
    - can be achieved in a relatively straightforward way by encryption and authentication protocols.
  - We want to prevent traffic analysis, direction finding, jamming and physical destruction.
    - Not as easy.

Protection Techniques for Communications Systems

- What can we do to prevent direction finding, jamming and physical destruction?

Attack	Protection
Physical Destruction	redundant dedicated lines or optical fibers
Direction Finding	highly directional transmission links, such as optical links using infrared lasers or microwave links using highly directional antennas and extremely high frequencies;
Jamming	low-probability-of-intercept (LPI), low-probability-of-position-fix (LPPF) and anti-jam radio techniques.

Spread Spectrum Communications

- A number of LPI/LPPF/antijam techniques go under the generic name of spread spectrum communications such as:
  - Frequency Hopping.
  - Direct Sequence Spread Spectrum (DSSS).
  - Burst Transmission.

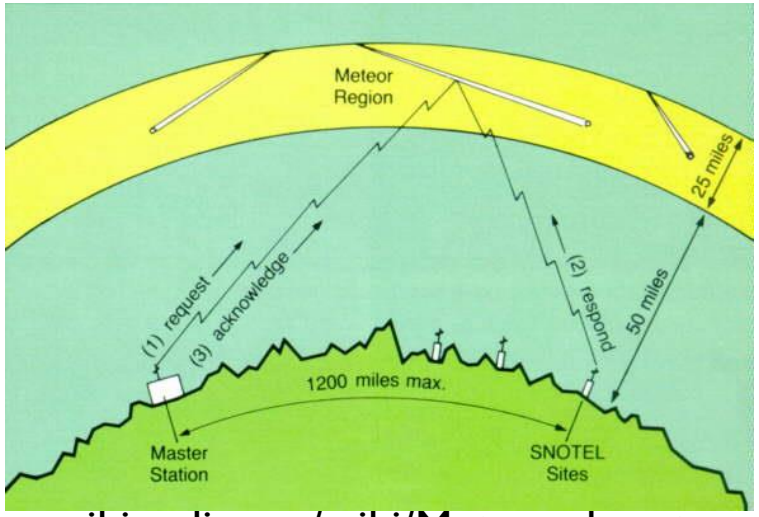
Frequency Hopping

- They hop rapidly from one frequency to another, with the sequence of frequencies determined by a pseudorandom sequence known to the authorized principals.
- Famously invented, over dinner in1940 by actress Hedy Lamarr and screenwriter George Antheil.

https://www.youtube.com/watch?v=Z0gu2QhV1dc

Burst Communications

- Meteor burst communications (MBC), also referred to as meteor scatter communications, is a radio propagation mode that exploits the ionized trails of meteors during atmospheric entry to establish brief communications paths between radio stations up to 2,250 kilometres (1,400 mi) apart.

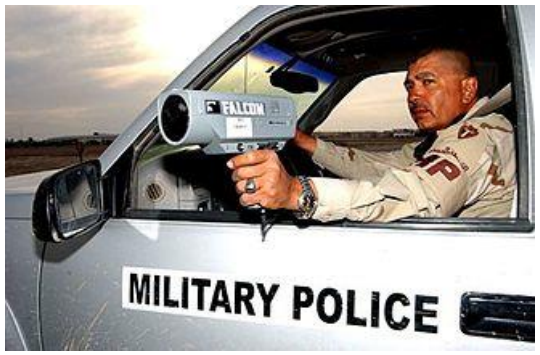


This relies on the billions of micrometeorites that strike the Earth's atmosphere each day

https://en.wikipedia.org/wiki/Meteor_burst_communications

Radars

- Search radar
  - A simple radar designs for search applications may have a rotating antenna that emits a sequence of pulses and detects echos.
- Doppler radar
  - Measures the velocity of the target by the change in frequency in the return signal.



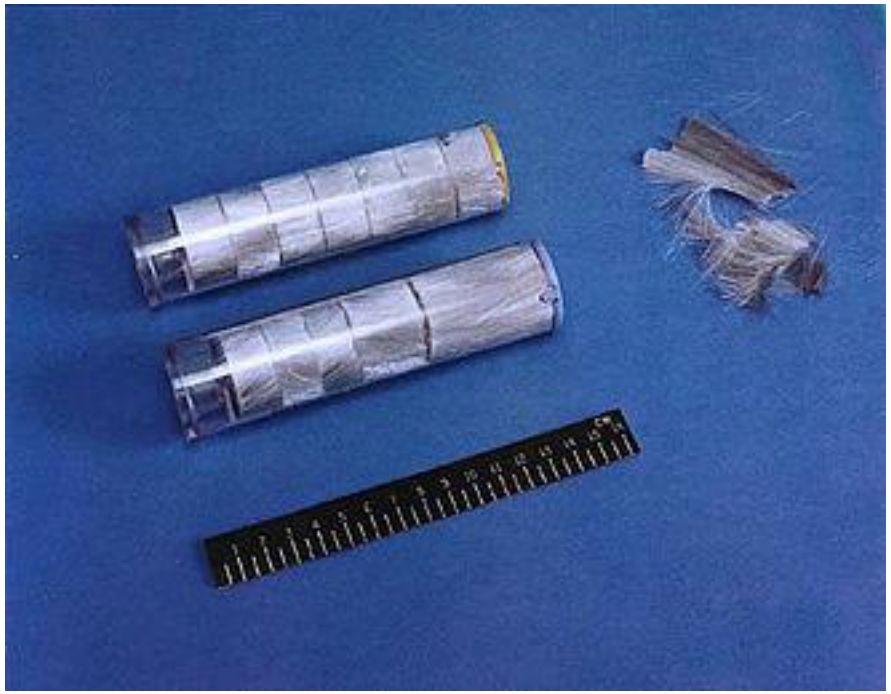
https://www.youtube.com/watch?v=d5T1vPmA-l4

https://en.wikipedia.org/wiki/Radar

Jamming Techniques

- World War 2
  - The earliest countermeasure to be widely used against radars was chaff.

Chaff, as in small aluminium strips (or wires) cut to one-half of the target radar's wavelength. When hit by the radar, such lengths of metal resonate and re-radiate the signal.

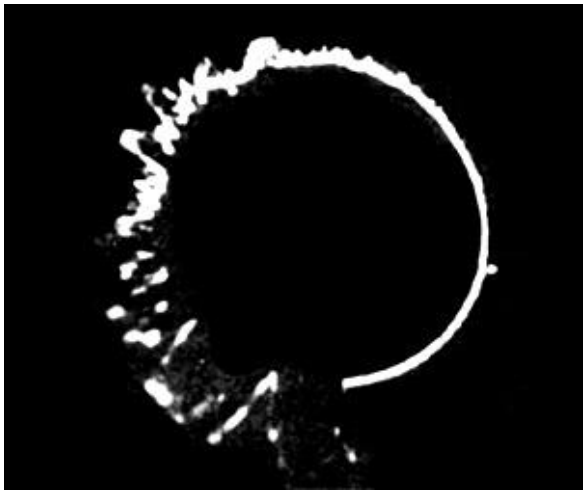


https://en.wikipedia.org/wiki/Chaff_(countermeasure)

Jamming Techniques

- Toward the end of World War 2, allied aircraft were dropping 2000 tons of chaff a day to degrade German air defenses.

A Lancaster dropping chaff (the crescent-shaped white cloud on the left of the picture) over Essen during a thousand-bomber raid.



The effect of chaff on the display of a Giant Würzburg radar. The effect of jamming appears in the left "jagged" half of the circular ring, contrasting with the normal "smooth" (unjammed) display on the right half of the circle, with a real target at the 3 o'clock position – on the jammed left side the real target "blip" would have been indistinguishable from the jamming.

https://en.wikipedia.org/wiki/Chaff_(countermeasure)

Directed Energy Weapons

- In the late 1930s, there was panic in Britain and America on rumors that the Nazis had developed a high-power radio beam that would burn out vehicle ignition systems. British scientists studied the problem and concluded that this was infeasible .
- They were correct — given the relatively low-powered radio transmitters, and the simple but robust vehicle electronics, of the 1930s.

Electromagnetic pulse (EMP)

- Things started to change with the arrival of the atomic bomb. Detonation of a nuclear device creates large currents giving rise to an electromagnetic pulse (EMP).
- Within a few tens of miles of the explosion, the radio frequency energy may induce currents large enough to damage most electronic equipment that has not been hardened.
  - The effects of a blast outside the earth's atmosphere are believed to be much worse (never been a test).
  - It is reckoned that most electronic equipment in Northern Europe could be burned out by a one megaton blast. For this reason, critical military systems are carefully shielded.

EMP

- EMP (from a single nuclear explosion) would do colossal economic damage, while killing few people directly.
- This gives a blackmail weapon to countries such as Iran and North Korea with nuclear ambitions but primitive technology otherwise.

What is I-war?

- NO … it is not what you think.

Information Warfare / Cyber warfare

- Information Warfare extends the electronic warfare doctrine of controlling the electromagnetic spectrum to control all information relevant to the conflict, by adding hacking techniques, and also incorporates propaganda and news management.
- This means the end result is to damage **critical infrastructures** and computer systems linked together within the confines of cyberspace.

Information Warfare –I war

- In April 2007, the government of Estonia had angered Russia by moving an old Soviet war memorial, and shortly afterwards the country was subjected to a number of distributed denial-of-service attacks that appeared to originate from Russia.
- Estonia's computer emergency response team tackled the problem with cool professionalism, but their national leadership didn't. Their panicky reaction got world headlines, they even thought of invoking the NATO treaty and calling for U.S. military help against Russia.

Stuxnet (2010)

- Unlike most malware, Stuxnet does little harm to computers and networks that do not meet specific configuration requirements.

BLACK CUBE®

A select group of veterans from the Israeli elite intelligence units that specialises in tailored solutions to complex business and litigation challenges

In April 2016, the company Black Cube employees Ron Weiner and David Geclowicz were arrested in Bucharest on suspicions of spying, phishing and cyber harassing the chief prosecutor of the Romanian National Anticorruption Directorate, Laura Codruța Kövesi and people close to her. The company denies any wrong doing saying that they were working under contract from the highest political powers in Bucharest and that "all of Black Cube's employees follow local law to the letter, and the allegations against them are unfounded and untrue". The Romanian government and Romanian Police denied the existence of any such contract.

http://www.blackcube.com/

https://en.wikipedia.org/wiki/Black_Cube

Summary

- Electronic warfare is an important pillar in any modern strategy of warfare.
- Electronic warfare and its extension in the form of (Information warfare) will continue to grow in prominence with the increased reliance on electronics both in the military and the private sector.
- In order to fully see the 'broad pic' in the vast subject of computer security, aspiring 'security people' will have to understand the principals of e-war ranging from the technical level up through the tactical level to matters of planning and strategy.

THANK YOU FOR YOUR ATTENTION!

ANY QUESTIONS?