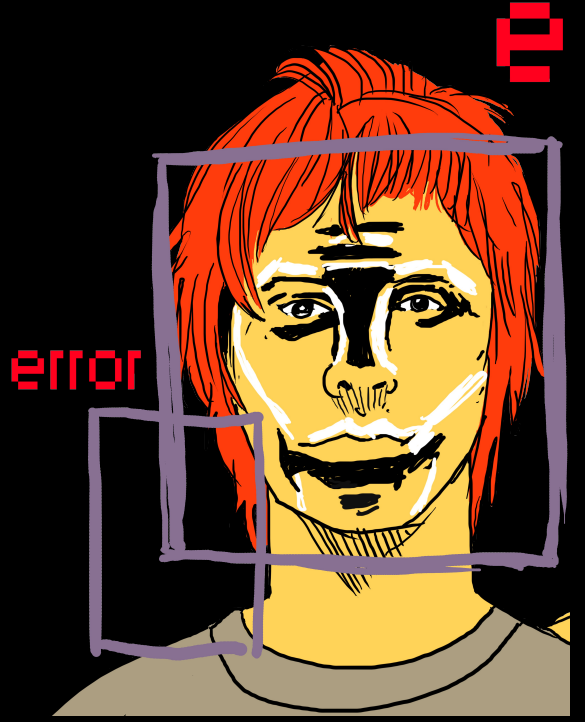
ARTICLE 19

Niels ten Oever
Head of Digital
Article19
niels@article19.org
nto@jabber.org
PGP : 8D9F C567 BEE4 A431 56C4 678B 08B5 A0F2 636D 68E9



Overview

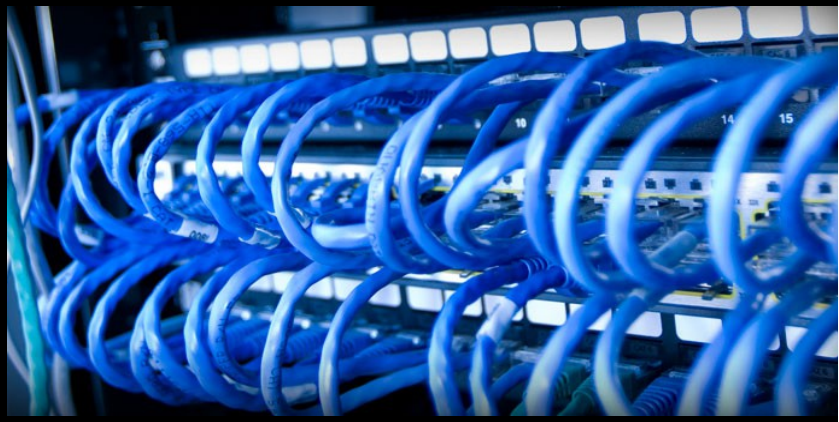
- What is systems security
- Adding Internet to the mix
- Infrastructure hacking
- Companies and governments
- Other infrastructure
- Cyberdefense and cyber offense

What is systems security

- Security is the state of being free from danger or threat
- Systems security is the practice of controlling which processes can be executed on a specific system, and by whom. It limits possibilities.
- Control, system transparency, autonomy and sovereignty
- Software, hardware & users.

Adding Internet to the mix

- What allows the Internet to be open and innovative is also what poses risks
- We're using the same infrastructure to do many different things at the same time.
- Who is responsible for what?



Adding Internet to the mix (RFC1281)

- The Internet is a voluntary network, operated on a collaborative basis
- Each participating network takes responsibility for its own operation. Service providers, private network operators, users and vendors all cooperate to keep the system functioning. Often on a best effort basis (depending on contracts)
- It is important to recognize that the voluntary nature of the Internet system is both its strength and, perhaps, its most fragile aspect.

Adding Internet to the mix (issues)

ARTICLE 19

- Privacy and security are important and recognized parts of the network on a protocol and standards basis.
- But it's only as secure as its implementation
- There are some issues (examples):
    - Confidentiality (heartbleed / SSL)
    - Integrity (packet injections / QUANTUM)
    - Availability (DDoS)
    - Leaky servers (passwords, ports, code)
    - Users
-

SCADA

- Supervisory control and data acquisition
- Type of industrial control system
- Bridges, power plants, water filtration plants, waste systems, electricity grids, gas and oil pipelines and refineries
- 99% of these systems are connected to the Internet. Why?
    - Unintentionally because of bad firewall settings
    - Because with the Internet, you don't need to build your own infrastructure

SCADA II

- The level of security is generally very low
- Many of the systems that were tested can be exploited with standard metasploit package
- Running on old machines. A lot still run Windows 2000, Windows 95, Windows XP (upgrade is expensive because of proprietary software (which has serious security implications)
- No hardware control (people plug in their own devices, use standard computers)
- Many of these systems are operated via webinterfaces

SCADA III

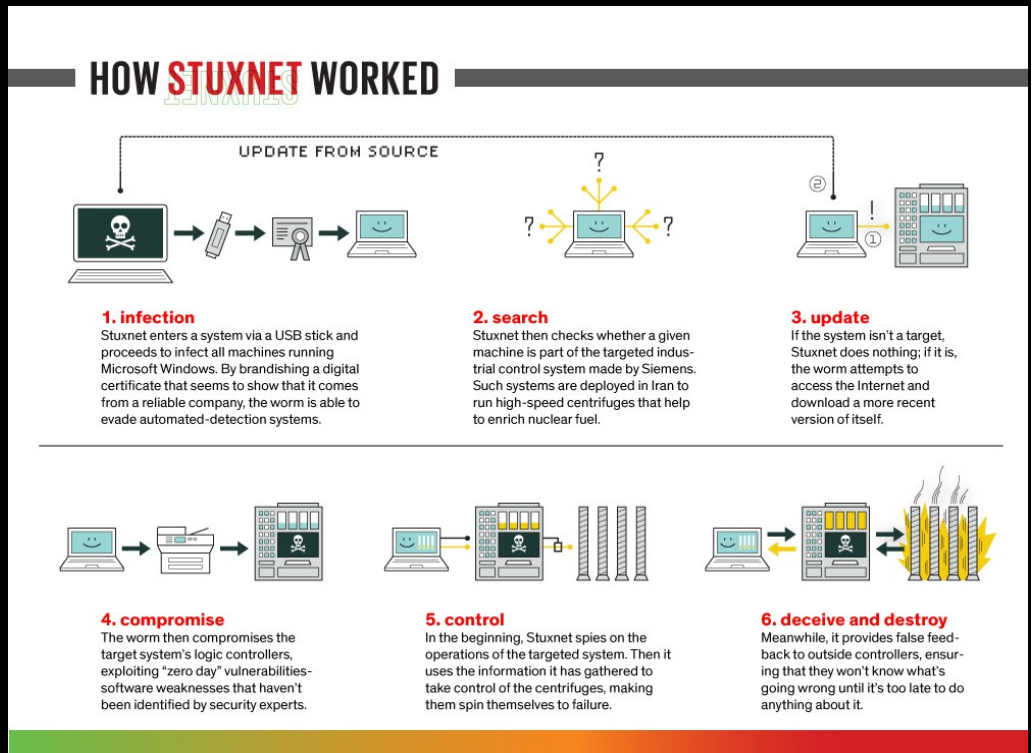
- Vulnerabilities are generally found by security researchers, also known as hackers
- Vulnerabilities are shared with big providers:
  - Siemens (by far largest S7 1200 PLC)
  - Emerson
  - Allen-Bradley
  - Rockwell Automation
  - Schneider Electric
  - General Electric

Companies & governments

ARTICLE 19

- Biggest attack to SCADA systems up to now was Stuxnet
  - Worm & Rootkit. Spread via USB device and via network.

  Country Infected computers
  - Iran 58.85%
  - Indonesia 18.22%
  - India 8.31%
  - Azerbaijan 2.57%
  - United States 1.56%
  - Pakistan 1.28%
  - Others 9.2%
-



Companies & governments

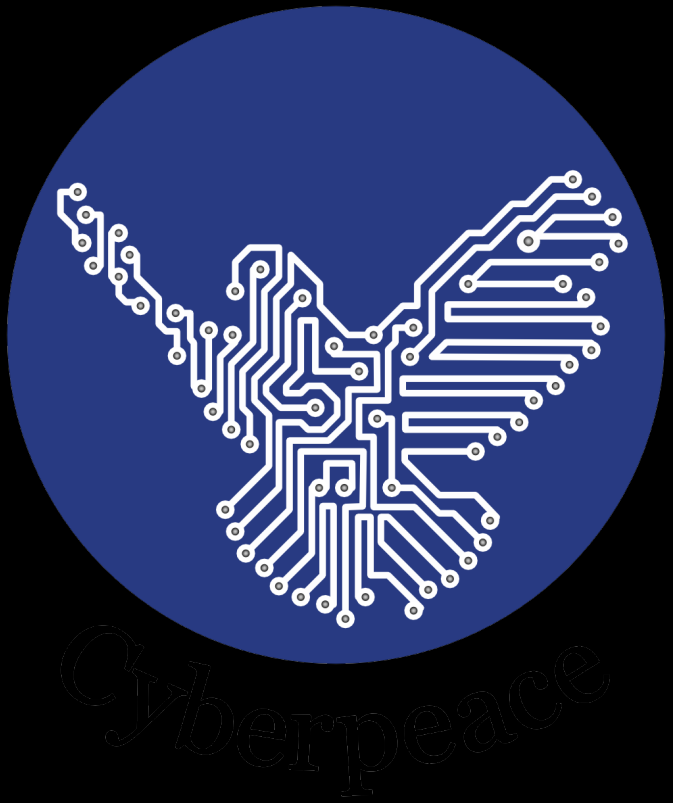
- Technology democratizes, once it's out there it can be use by, and against, everyone. It's not a precision tool.
- Malware is copied and recycled.
- Governments work together with companies because they don't have the in-house capacity. Companies do not have the same accountability levels
- Hacking team, Blue Coat, Gamma International, Trovicor

Other infrastructure

- Border Gateway Protocol
- Domain Name System
- Undersea cables
- Standards
- Providers (Google, Apple, Cisco, etc)

Cyber defense & offense

- Technology democratizes, once it's out there, you cannot get it back
- Defense is still poor, increased capacity is needed. For instance institutionalized penetration tests of infrastructure
- Attribution is a very big problem and risk > Sony
- CIRTs and CSIRTs can help, but this is reactive (the house is already on fire)
- These attacks *always* impact civilians and the Internet



Cyberweapons do not solve cybersecurity
improved security practices do