Cybersecurity and space sector

Philippe Gaucher – ANSSI

October 12th, 2017

SIRIUS'17

Agenda

1. ANSSI in a nutshell
2. Examples of modern threats to HVT
3. French approach to Critical Information Infrastructure Protection (CIIP)
4. Application to the space sector

ANSSI in a nutshell

ANSSI

- French cybersecurity and cyberdefense agency and authority
- Interministerial position, under the prime minister
- Created in 2009, now with 500+ people, growing

Scope

- Originally government and critical infrastructures operators
- Extending to SME, citizens, etc.

Fields of action

- Operational matters (CERT-FR)
- Expertise, R&D
- Secure information systems
- Evaluation, certification, regulation, training (MOOC)

Current priorities

- Critical Information Infrastructure Protection (CIIP) law (« LPM* »)
- Cybersecurity industry policy

*LPM: French Military Planning Law includes CIIP articles.

Modern threats against High Value Target

> Advanced Persistent Threat

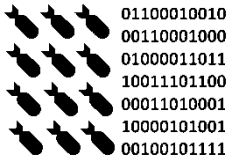
- Specific targets and precise goal
- Custom and mutliple tools and ways of
- Like a military operation (OODA)
- Long term objectives

> Goals

Espionage

Sabotage

Neutralization

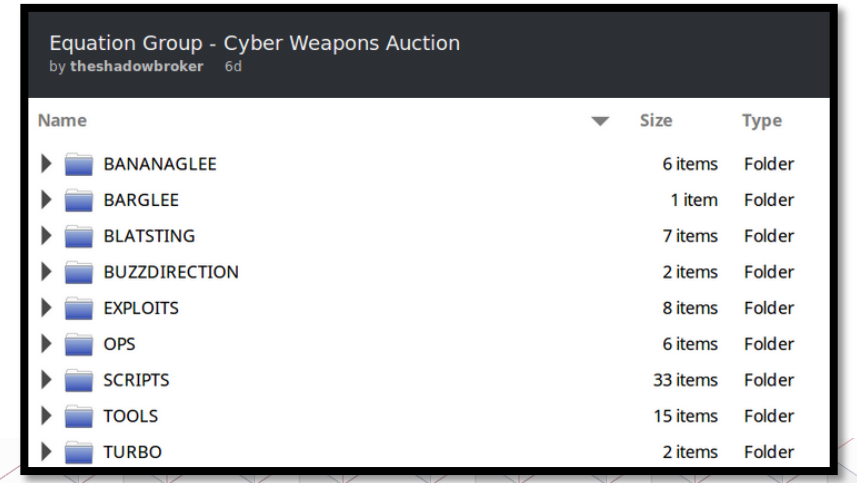


Reputation

Modern threats against High Value Target

- Proliferation of high-level tools
  - Snowden
  - Vault7
  - Shadow brokers

- Tools
  - More and more complex
  - More and more handy



The French CIP approach

- CIP: critical infrastructure protection
  - Defense and national security approach
- Key concept: **critical infrastructure operators***
  - "*An operator whose unavailability could strongly threaten the economical or military potential, the security or the resilience of the Nation*"
  - Approx. 250 CI operators: 40% public, 60% private designated since 2006
  - 12 sectors: health, water, defense, **Space,** transportation, finance, etc.


Power


Food


Finance


Public

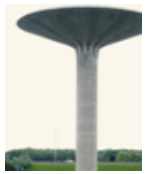

Telco


Health


Industrie


Defense


Transport


Water

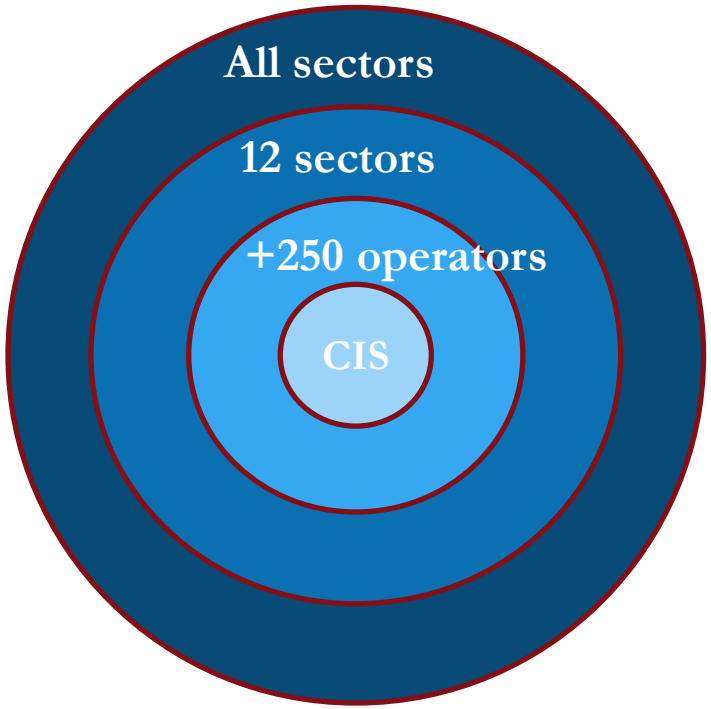

Space & Research


Justice

*OIV in French, standing for operators of vital importance

The French CIIP approach

- CIIP: critical <u>information</u> infrastructure protection
  - Complete the CIP approach with a focus on IT systems
- Key concept: **critical information system***
  - Information systems *"whose unavailability could strongly threaten the economical or military potential, the security or the resilience of the nation."*
  - Requirements of the CIIP law exclusively apply to these information systems
  - Operators are responsible for identifying their critical information systems and provide ANSSI with a list.



*SIIV in French, standing for information system of vital importance

CIIP law – LPM*, article 22: 4 main CIIP measures

> Mandatory security rules: organizational and technical

- 20 rules, adapted but **mostly similar across business sectors**
- Examples: IT security policy, documentation, network mapping, security maintenance, etc.
- Prescribe the use of qualified providers (IT incidents detection & response, audit)

> Incident notifications to ANSSI

- Great importance of trust and confidentiality

> Inspections of critical IT systems

- ANSSI can mandate audits, executed by ANSSI or by *qualified* private auditors

> Major crisis

- ANSSI can mandate measures in case of crisis

*LPM: French Military Programmation Law, includes CIIP articles.

Cyber threat assessment in space sector

- The ministerial sectorial order
  - Published 8th September, 2017
  - Specific IT systems typology
  - Adresses protection to known attack vectors & tactics + defense in depth
  - Enforces good practices

- Regulation or incitation ?
  - CIIP is complementary to threat assessment
  - CIIP law forces good practices and inspections on critical IT systems of operators of critical infrastructures only
  - ANSSI qualifies IT security hardware, software and service providers

Thank you for your attention

Philippe.gaucher@ssi.gouv.fr