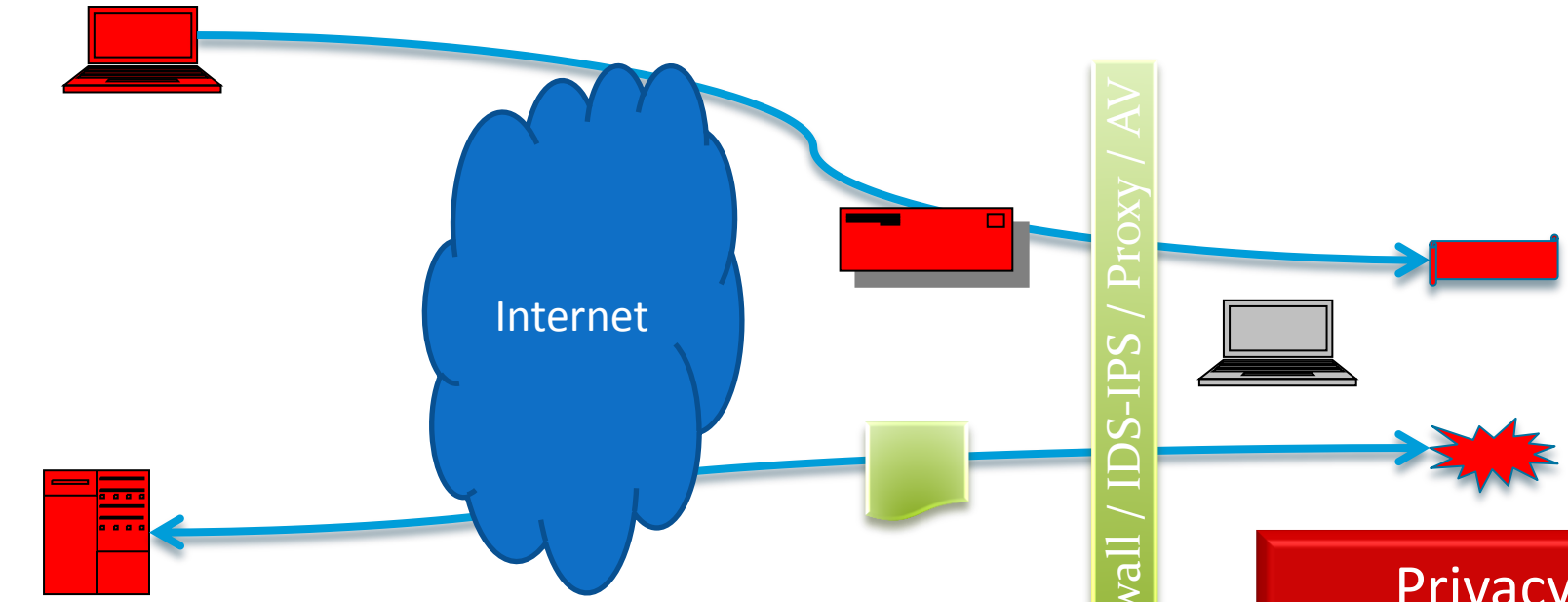
Elementen van de Belgische cyberdefense (military)

LtKol De Bruycker, Infosec & Cyber Defence,
Algemene dienst Inlichtingen en Veiligheid

Cyber Attack?

- A Cyber Attack is deliberate action
  - to **disturb the proper functioning** of an ICT System. (Denial Of Service)
  - to **intrude** into an ICT System and
    - read, change, inject of delete information (espionage)
    - misuse its abilities

Intrusion impact



CC Server

Full Control

- Mails
- Files
- Key logger (passwords)
- Social media
- Surf behavior
- Microphone/web cam
- …

Privacy
Freedom
Economy
Sovereignty
Operationality

Cyberdefense

Protection of our “own”

Networks & systems

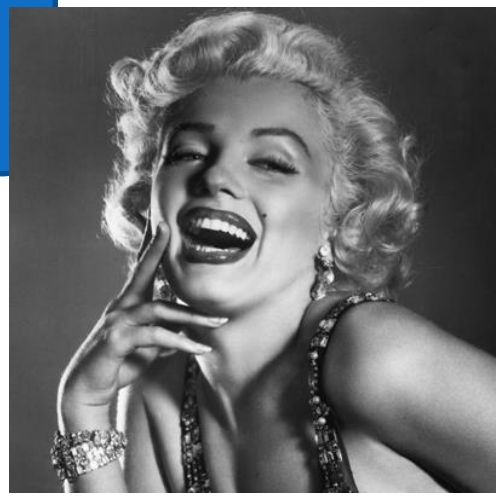
Against cyber attacks

What do we need?

More rules or laws

- Probably yes, but..
  - Laws only help if you can enforce them
  - Laws hinder the defender and don’t stop the attacker …

If I'd observed all the rules,
I'd never have got anywhere

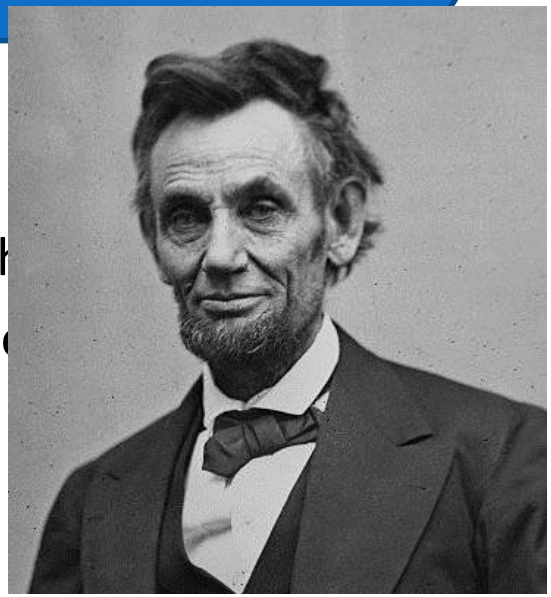


Cyber deterrence

- **D**

> The probability that we may fail in the struggle ought not to deter us from the support of a cause we believe to be just

- the retaliator must
  - Have the means to react
  - Convince the aggressor th
  - Prevent collateral damag



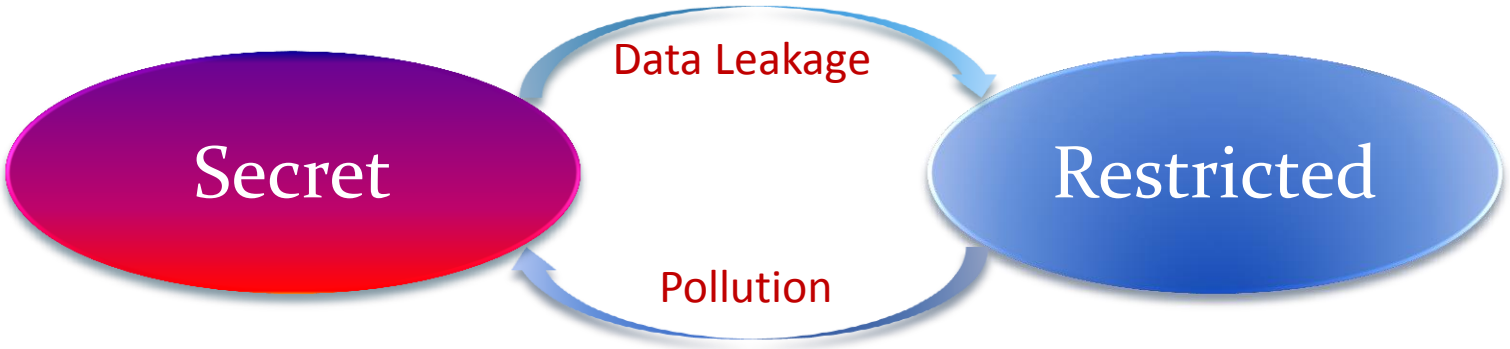
Collaboration

- It takes two to tango
  - Trust
  - Win-Win
- Exposure risk
  - Knowledge proliferation
  - If you know what I can detect, you also know what I can't
  - Technology advantage (**single use** weapons & expiration date)
- You can own weapons, but what about people?
- It's hard to talks about incidents, detection technologies…

A launch a cyber attack against B
B have no cyber capabilities to respond
B retaliates with …

Protect CIS

- Knowledge & Awareness
  - Users & management must be aware of the risks
- Secure systems
  - *Yes we can* seriously improve security with limited extra cost
  - Build-in security (by design)
  - Integrated security & vulnerability management (BYOD)
  - Military grade security networks!
  - Multi-domain & multi-level secure gateways



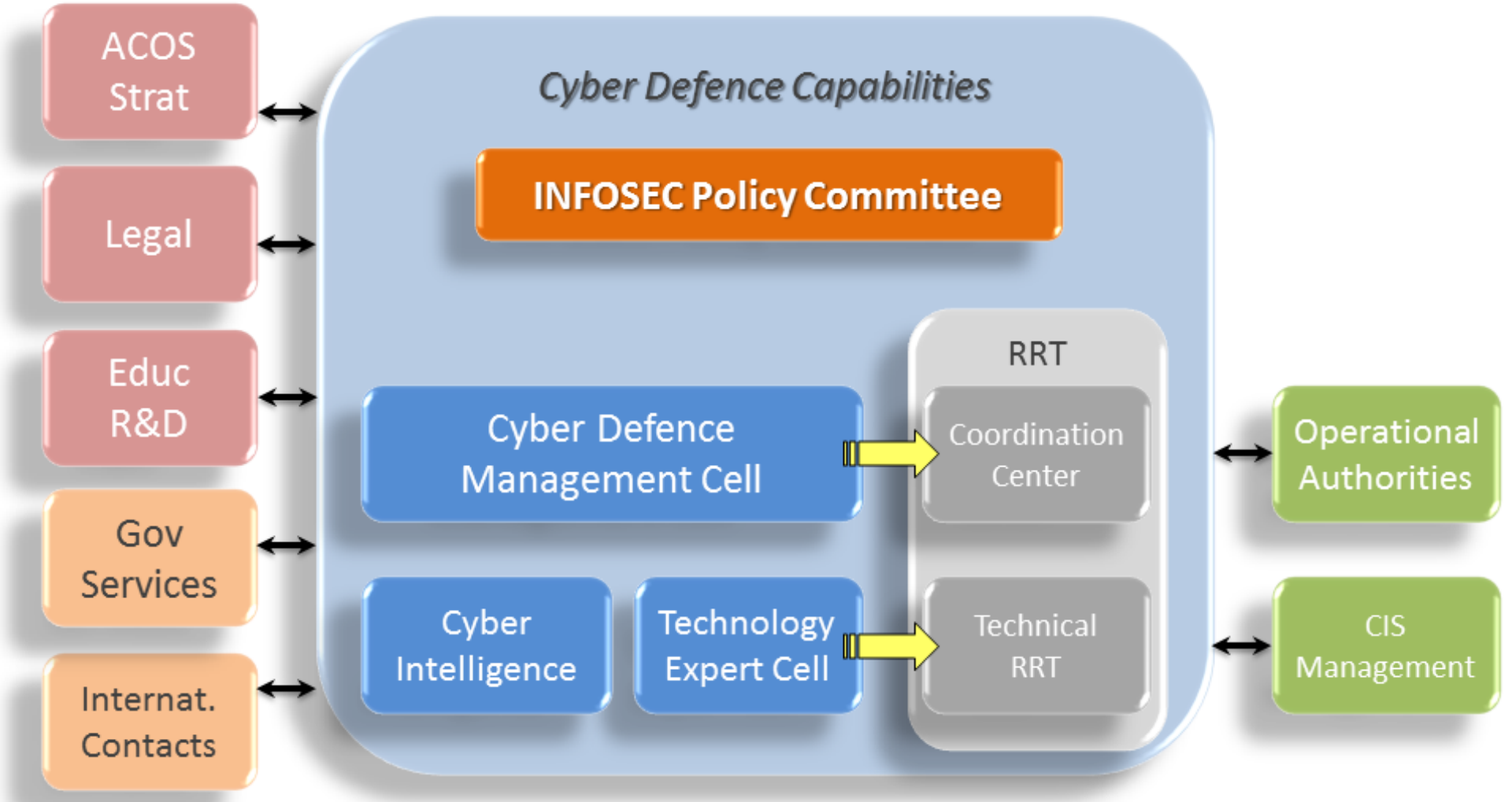
Detect

- Network monitoring
  - Intrusion Detection Systems
  - Cyber Security Operations Centres (SCOC)
- Advanced detection techniques
  - Non signature based
- Technical information exchange (intrusions)

Respond

- *Reach out to official services*
- Incident handling processes
- Malware analysis
  - Automated & through collaboration
- Digital forensics

Belgian Defence - Cyber Defence Architecture



Questions?