

A threat to ICT-based safety systems

Information Operations



TNO Physics and Electronics Laboratory



Eric Luijff, Principal Consultant



Content

- **Information Operations**
 - history
 - definition & goal
 - what does it mean for you?
- **ICT-attacks**
- **Critical infrastructures and Safety critical systems**
- **Questions**



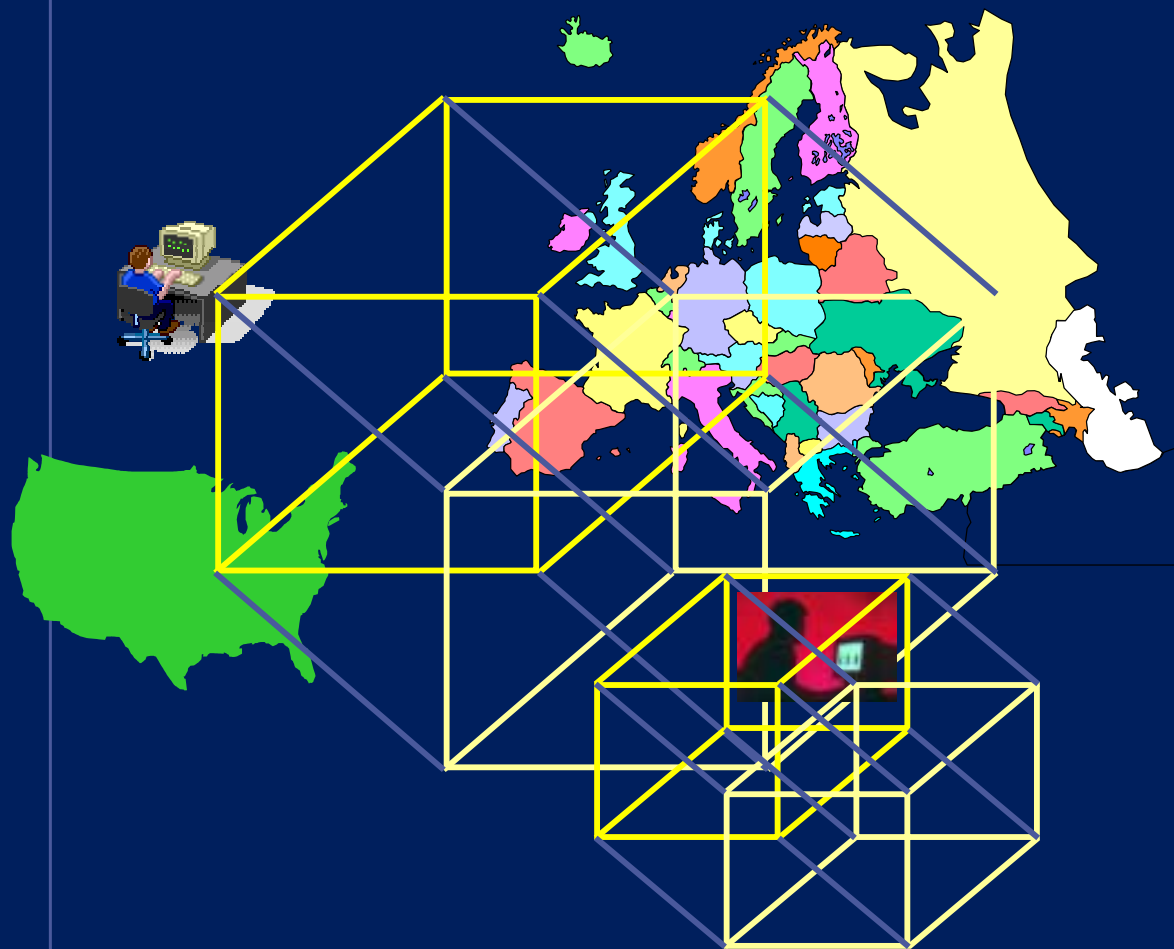
Cyberspace, the 5th dimension

Land, Sea,
Air, Space

Cyber threat

Up-link in the
Sahara is closer to
you than the bakery
around the corner

FBI 9/2/2001: Ukraine hackers collected
information about 1 million credit cards



Information Operations

INFORMATION &
ICT-SYSTEMS

as

TARGET

MEANS

&

WEAPON



Information Warfare => Information Operations

- **Sun Tzu (500 BC)**
- **Visionaries about information age warfare**
 - Tofflers Third Wave 1980
 - Cyberwar is coming (1993), Arquilla & Ronfeldt
 - What is Information Warfare ? (1995), Libicki
- **Information Warfare in 1999**
 - too sensitive as well as incorrect term => Information Operations
 - now: IW library-term & Info Ops part during conflict



Information Operations

- **GOAL: influence decision makers**
 - [in support of political and military objectives]
- **by**
 - **affecting**
 - **exploiting**
 - **protecting**
- **of**
 - information
 - information-based processes
 - C2 systems
 - CIS

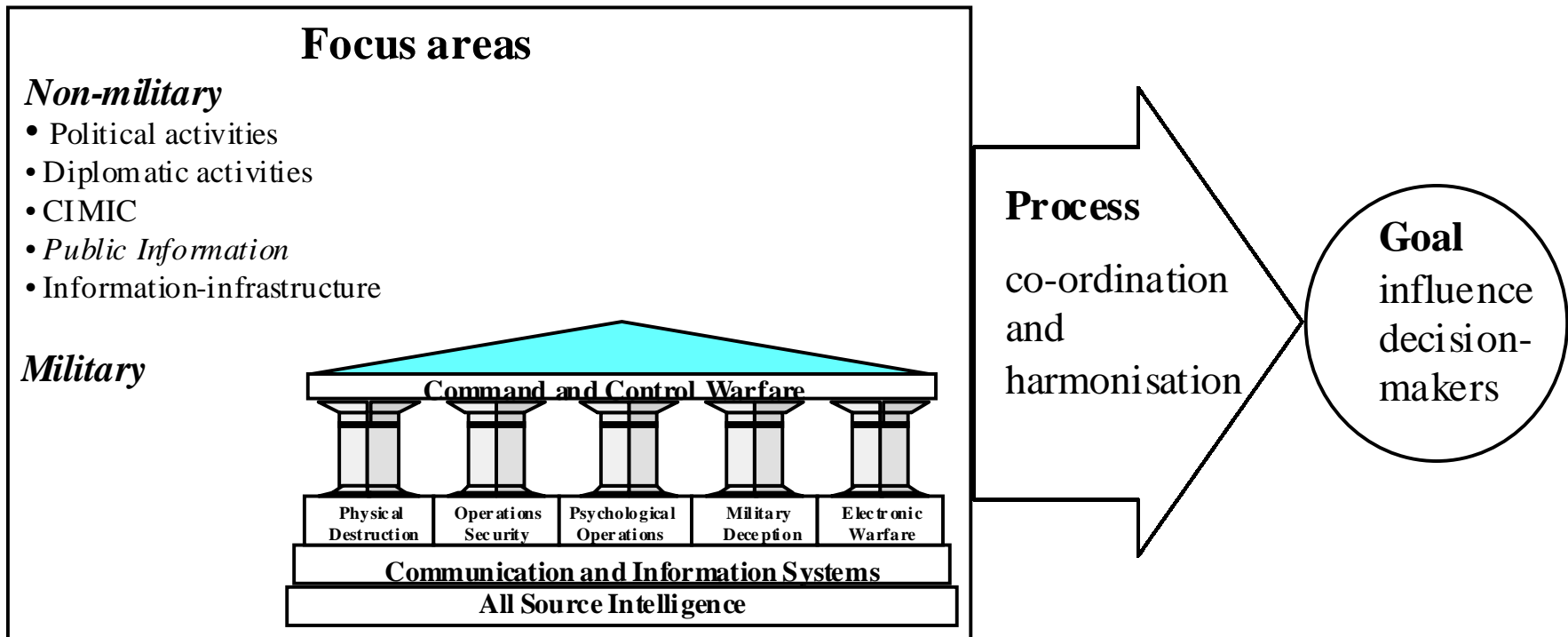


Information Operations

(figure from NL policy)

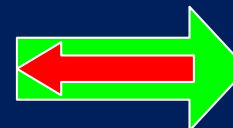
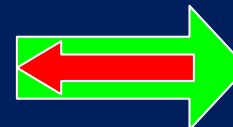
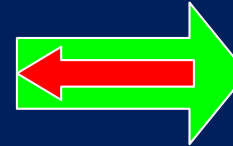
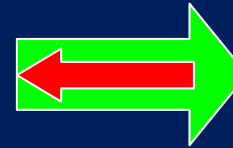
Political and military objectives

Information Operations



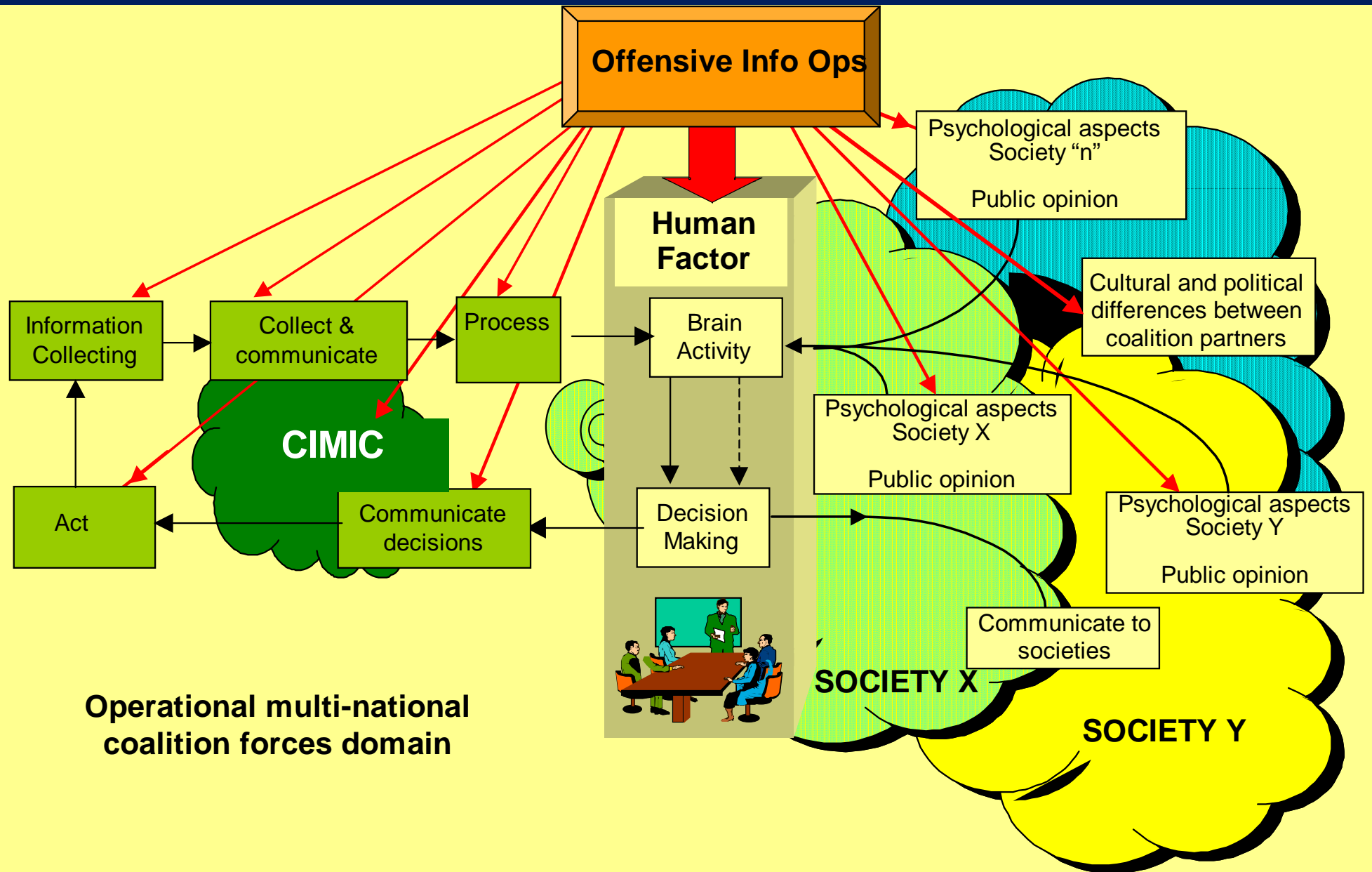
Info Ops co-ordination & coherence

- Military movements / actions
- Diplomatic activities
- Public information (world)
- PsyOps - local people
- Single-minded coalition
- Support by own citizens
- CIMIC



One single,
communicated
coherent
message

Info Ops: Society can be target



Information Operations

- **Recognises**
 - psychological effects
 - non-state actors
 - transnational actors (e.g. supporters, activists, terrorists)
 - asymmetric threats

- **Threats to society at large**
 - critical infrastructures
 - critical functions
 - **safety critical systems**

ICT-attacks

who and why?



Attackers and reasons

Low End



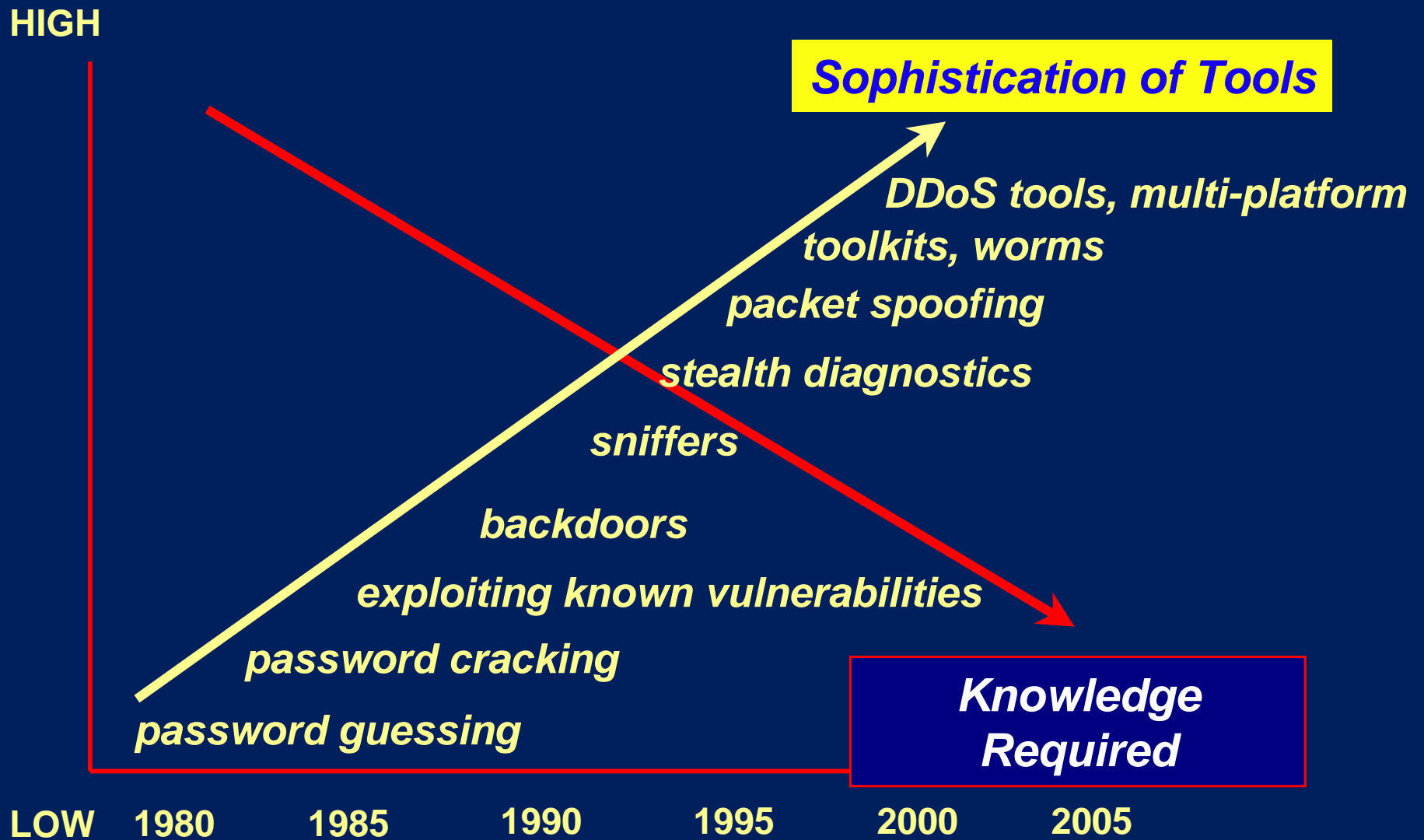
- Recreational hackers
- Script-kiddies
- Curiosity; bragging
- Hack-miles
- Cyber-graffiti

Fast application of last patches decreases threat largely

Annoyingly, this counts for 90-95% of the external 'threats'



Sophistication of tools versus knowledge requirements



Attackers and reasons

Low to High End

- **Virus creators**
 - “Fun”, disappointed love,...
- **Trojan creators**
 - Unknown of consequences to deliberate damage

High financial losses by Melissa, I-L-Y, NIMDA, ...



I-LOVE-YOU



Snits / Sneek



BT & Deutsche Bank services down

Attackers and reasons

Mid level

- Professional hacker
 - Financial gain
- Information broker
 - Economical gain
 - Information (spy)
- Criminal
 - Financial gain
 - Frustrate crime investigations

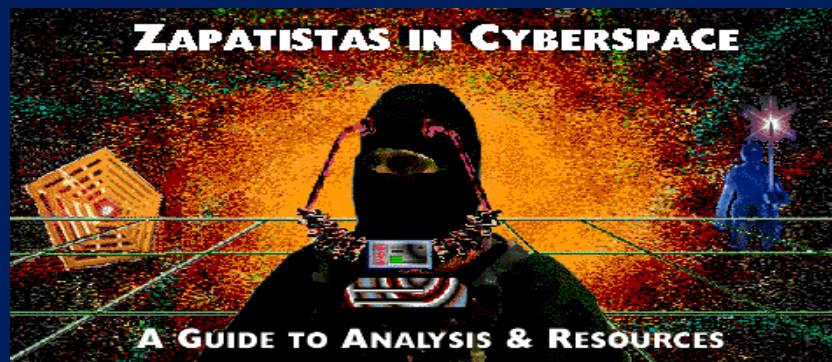


The silent partners ..

Attackers and reasons

Mid level

- **Activist**
- **E-sit-ins**
- Media attention
- Visible demonstration
e.g. denial-of-service attacks
- Put pressure on **you** as target



Attackers and reasons Mid to High End

**Fluffi Bunni
goes JIHAD!**



- **Hacktivist**
- **Activism with high impact and no consideration for losses or harm to people**

Part of the E-tifada, Kosovo-war, India-Pakistan, China-Japan, Armenia-Azerbaijan, China-Taiwan, anti-globalists (e.g. WTO)

EM-spectrum threats
ICT-based threats



E-tifada

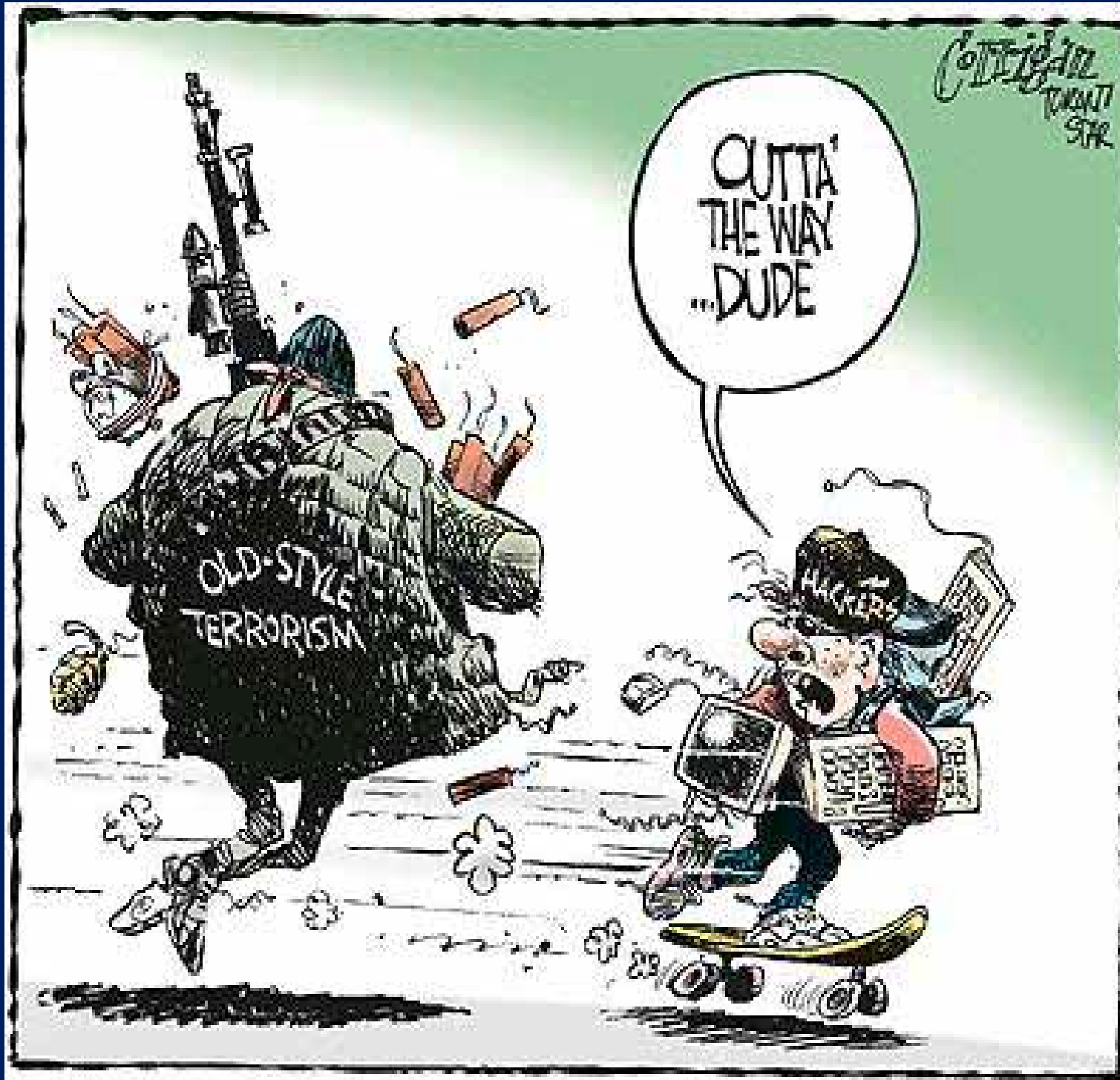


Attackers and reasons

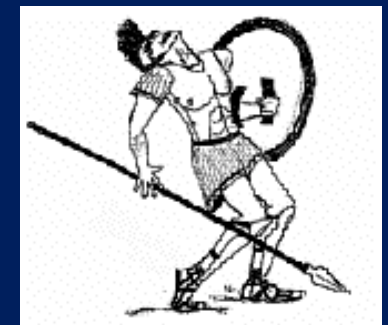
High End

- Military & 'secret services'
 - **Information Operations ("Cyberwar"-part)**
 - **Cyber terrorists**
 - Not seen yet
 - PIRA and OBL intentions ...
- Info dominance
 - Intelligence collection
 - Intelligence collection
 - Deny freedom to act and decide
 - Influence decision-maker
 - Counter-attack
 - Maximise damage to & disturbance of infrastructures, persons, society
 - still like the big bang, but...





ICT threats for (Safety) Critical Infrastructures



What's at Stake ?

Military

C4I

Power grid

**Civil
Defense**

Water pumps
& sewage

Vital human
services

Telecommunications



Mass Media



Finance

**Information
Infrastructures**

Transport

Industry

DAILY INCIDENTS

**Hacktivists, Cyber
terrorists, IW**



Threats

- Acts-of-God
- Nature
- Technology error
- Human error
- Deliberate attacks & disruption

Two paradoxes

(Stroomloos, Rathenau Institute)

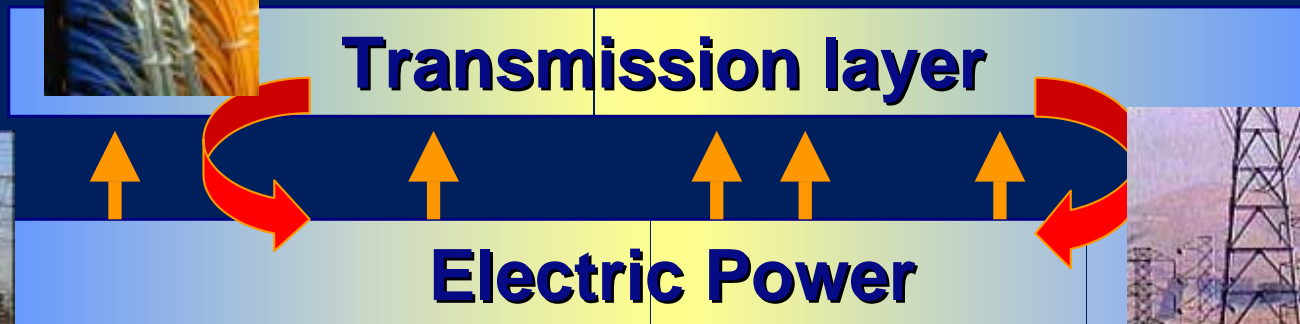
- The less vulnerable a country is with respect to infrastructure services, the more each disturbance thereof hits society
- At the same time, society will increasingly use such a service because it seems to be so reliable (perception)



Building on top of an unreliable basis?

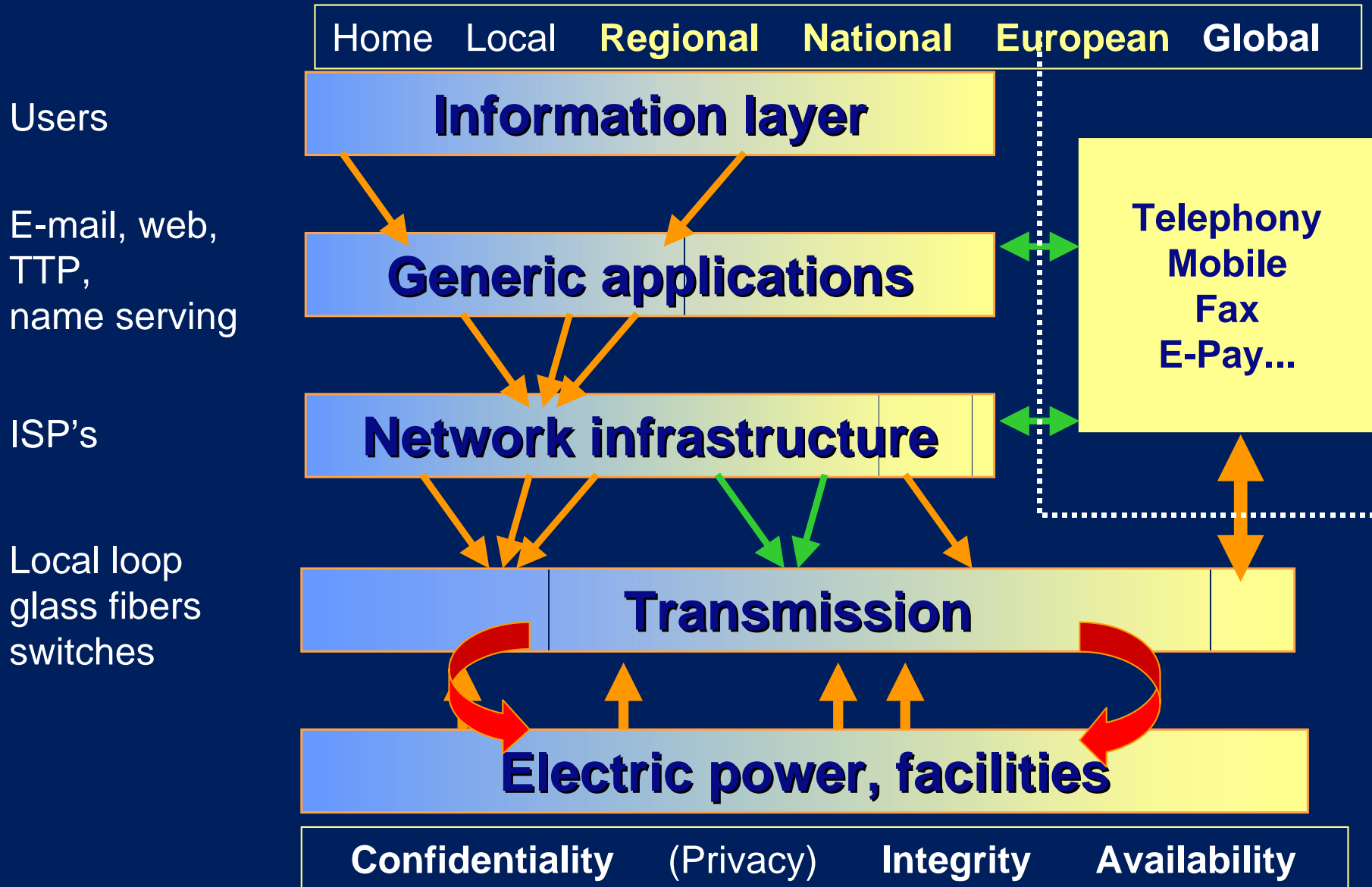


local loop
glass fibres
switches

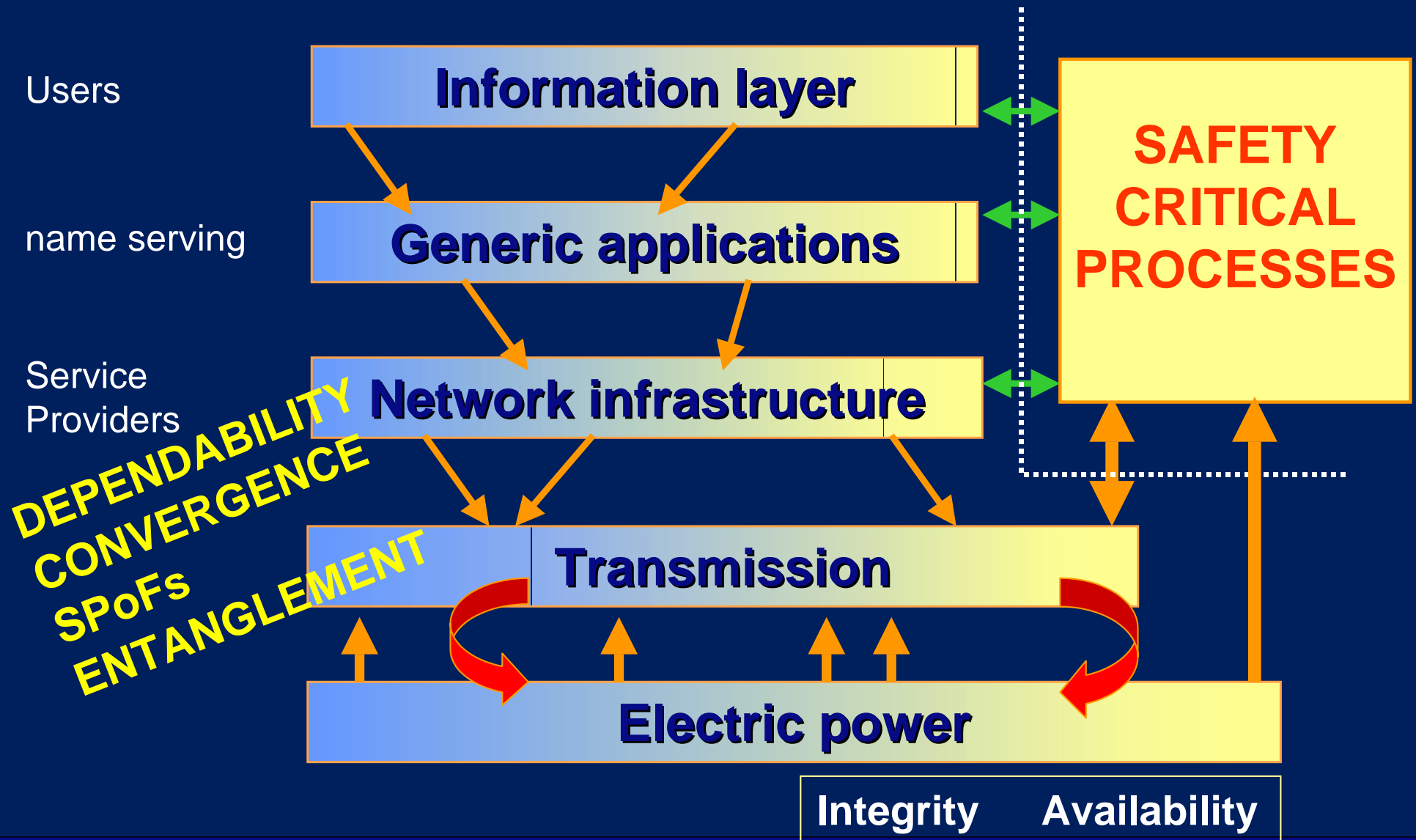


Vulnerability assessment model

(NL-study KWINT - Internet vulnerabilities)



Increasingly interconnected



Example: electric power industry is vulnerable

- **No guarantee that controlling ICT cannot be hacked (e.g. US; Norway)**
- **Foreign hacker roamed in Californian power control system for 17 days**
- **Liberated European power generation / consumption market uses Internet as trading place**
- **ICT requires tremendous amount of power**
 - 60-100 MW/data hotel; power cable consumption overload
- **UK: guard shuts down doors nuclear power plant**



Safety critical systems

- Increasingly use Commercial-off-the-Shelf (COTS)
- Less “bio-diversity” causes higher risks
- Increasingly remote control & maintenance: risk of backdoors
- Lack of security baselines for this segment (see GSI initiative)



Critical Infrastructure Protection (CIP)

The process

- **Awareness about**
 - threats and risks
 - dependability, convergence, entanglement
- **Vulnerability & dependency assessment** (ISO 17799...)
- **Take balanced protective measures**
- **Maintenance of protection !**
 - overlooked by management
- **Caveats**
 - threats change with the high dynamics
 - fast infrastructure developments



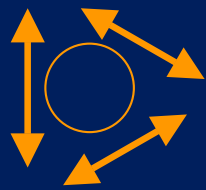
Assurance aspects to consider

COTS risks & technology watch

Intrusion detection

Infometrics & incident response

Investigation & legal action



Information collection on whom/why

Business Continuity (fast recovery)

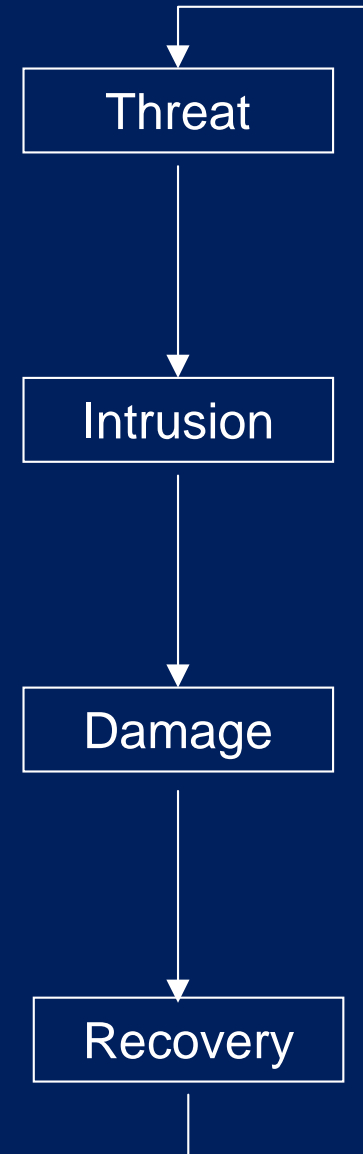
prevention
reduction

detection

reaction

correction

evaluation



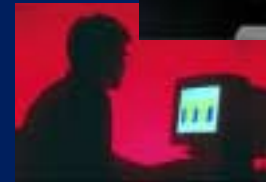
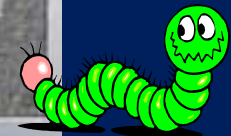
Intruder Team

CERT

Conclusion & input for discussion

- **Information Operation sets the mind for**
 - (safety) critical infrastructure protection
 - new threat scenarios with ICT as our/your Achilles string
- **Safety critical infrastructures**
 - increasingly interconnected & dependent on ICT-infrastructures
 - increasingly vulnerable
 - society increasingly relies upon them & expects safety
- **Action required**
 - investigate and become worried...
 - consider low probability / high impact as well
 - remedial actions should be structured and balanced

Questions?



Email: luijf@fel.tno.nl
<http://www.tno.nl/instit/fel/infoops>



TNO-FEL's URLography

- Critical infrastructures and “Cyberwar”
 - <http://www.tno.nl/instit/fel/infoops>
- Information Security
 - <http://www.tno.nl/instit/fel/infosec>
- Articles via
 - <http://www.tno.nl/instit/fel/intern/wkisec16.html>
 - <http://www.tno.nl/instit/fel/refs>
- Contact: luijf@fel.tno.nl

