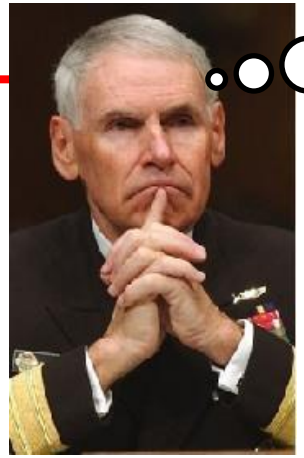
Cyberdefence as Building Block of the Austrian Cyber Security Strategy

Cyberstorm
22. October 2014

Cyber Domain

Basic Values
Confidentiality
Availability
Integrity
Of ICT-Systems,
Consisting of
Infrastructure
HW, SW, Buldings
Data, Information,Knowledge
Organisation, Personnel

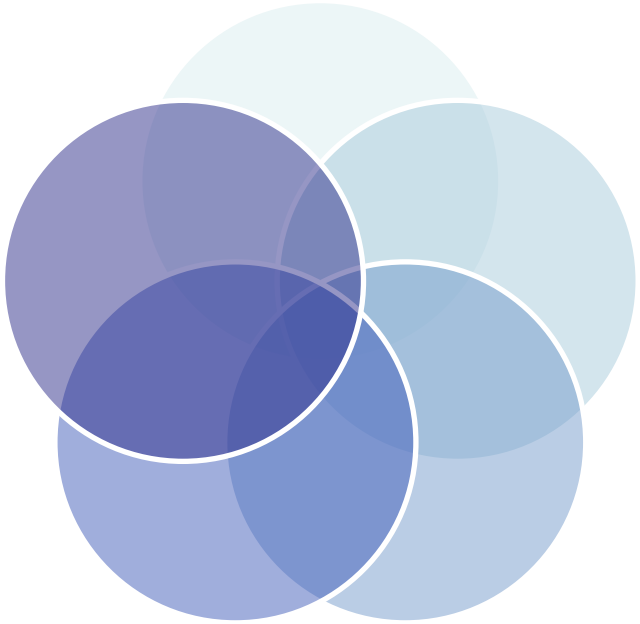
Areas of Operation



Airspace

Cyberspace

Land



Space

Sea

Cyberspace

Character

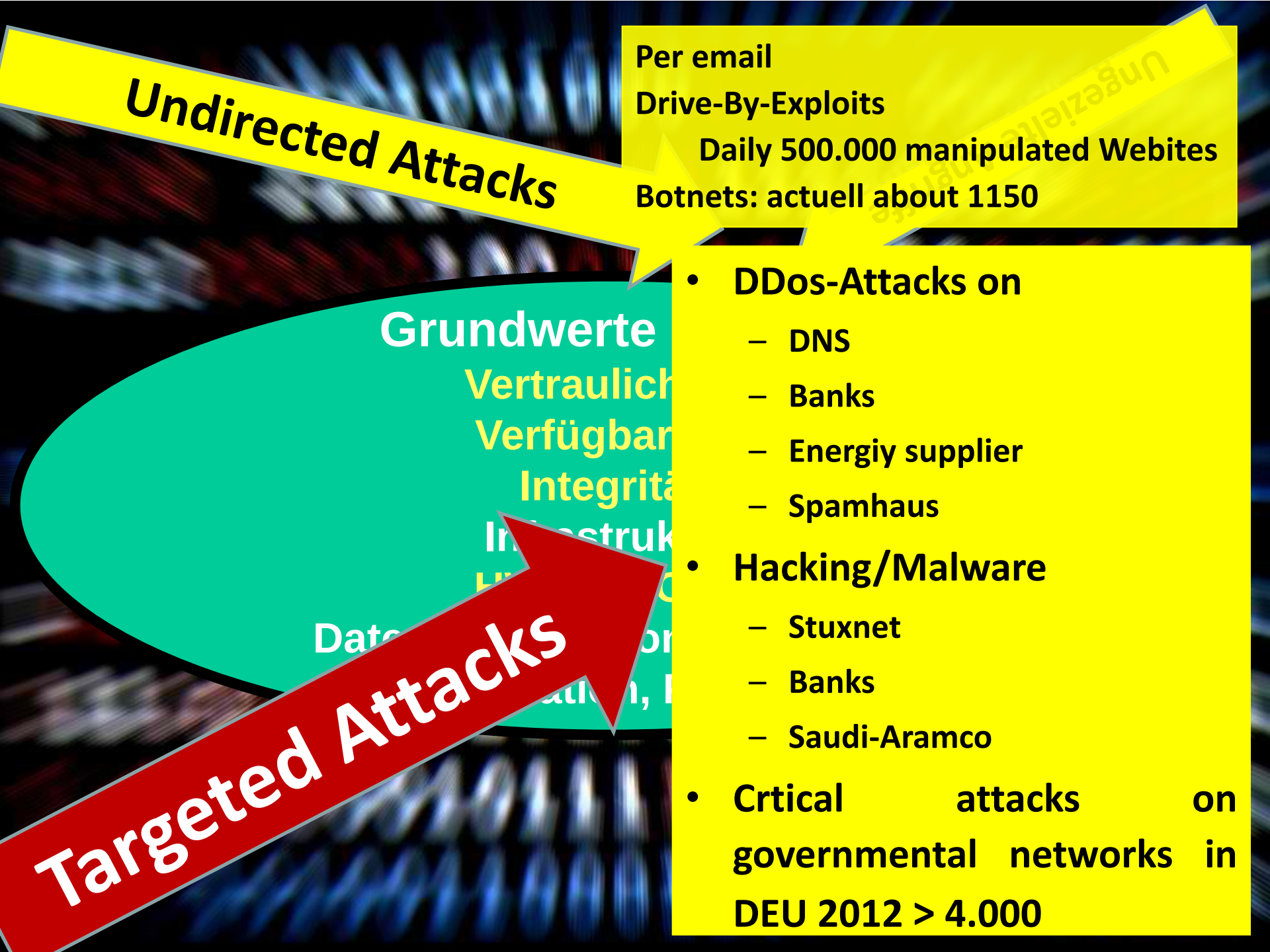
- Playground
- Action area
- Crime Scene
- Battlefield/ Theatre of War

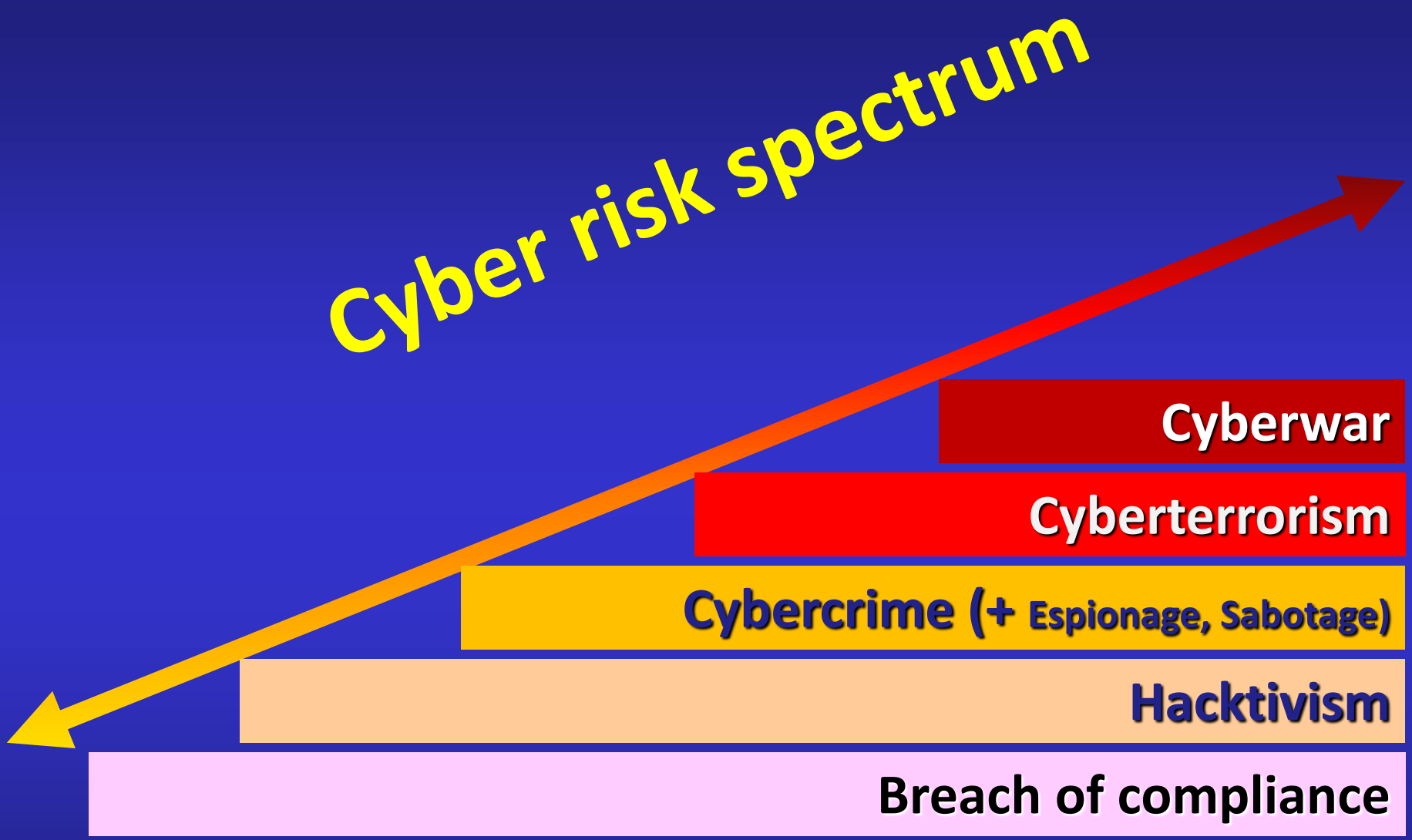
Actors

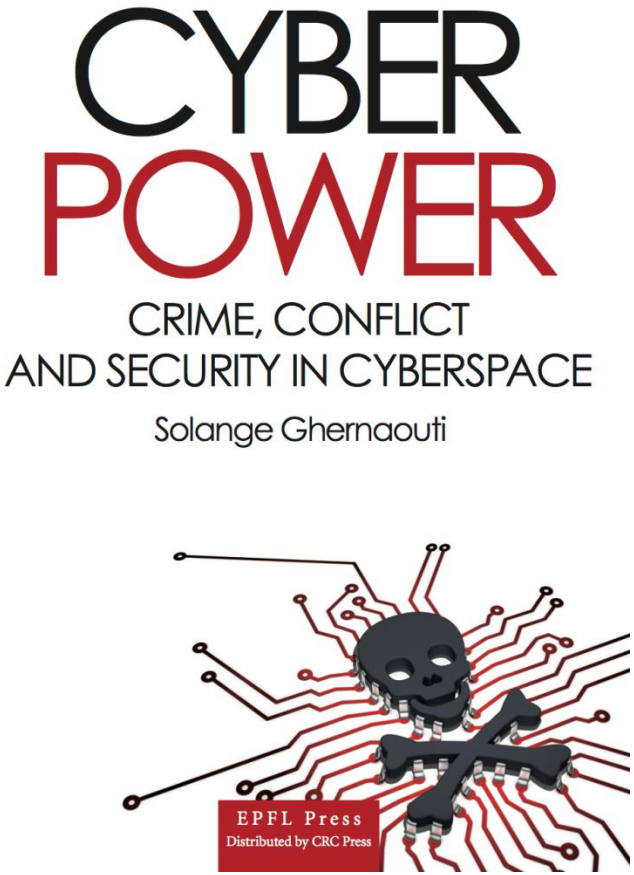
- Script Kiddys
- Activists
- Cyber Anarchists/ „Vandals“
- Criminals
- Cyber Spies
- Cyber Terrorists
- Govermental „Cyber Warriors“

Differentiation

- Motivation
- Objective Targets
- Ressources
- Capabilities

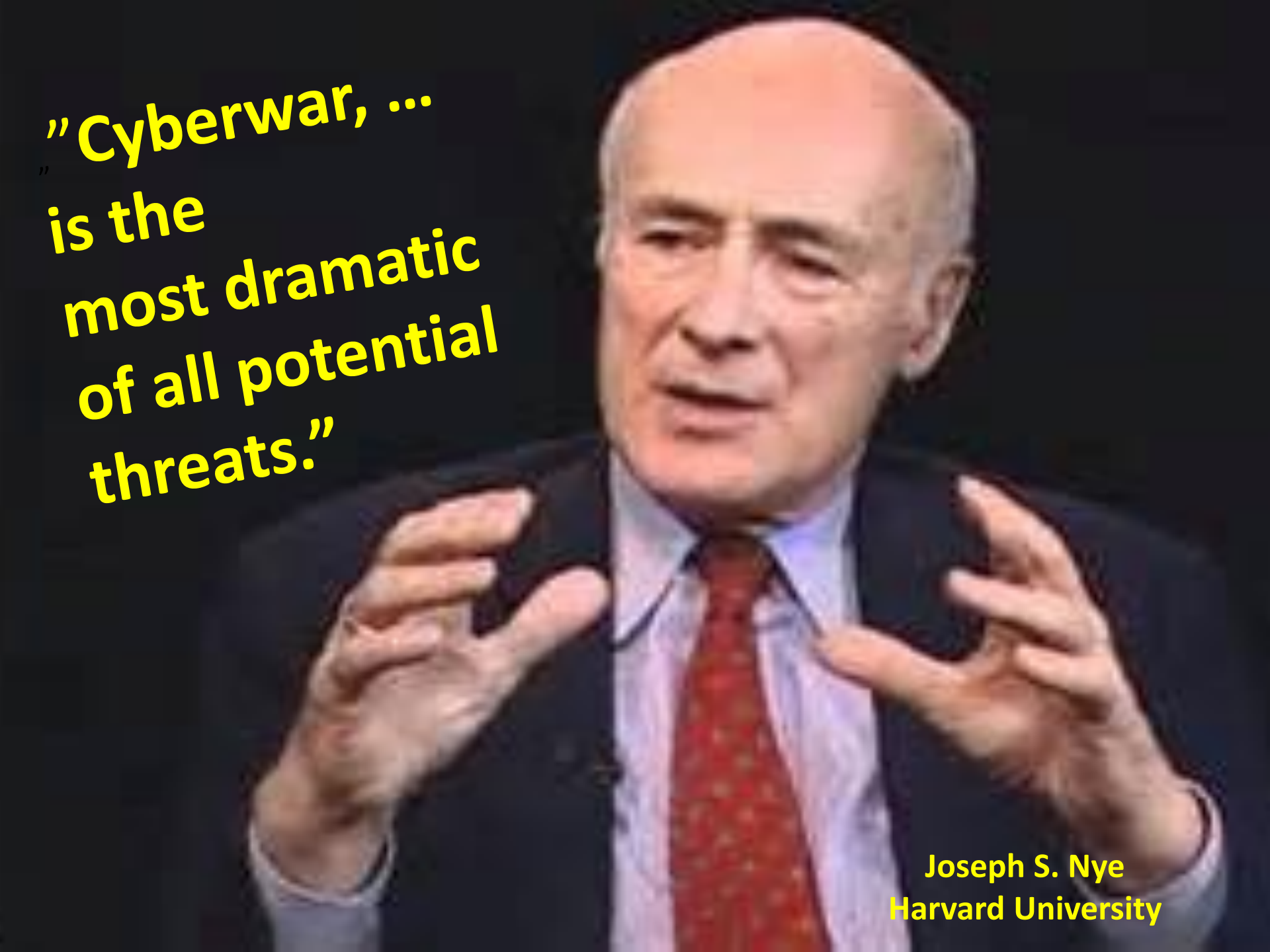

Undirected Attacks
Per email
Drive-By-Exploits
Daily 500.000 manipulated Webites
Botnets: actuell about 1150
Grundwerte
Vertraulich
Verfügbar
Integrität
Targeted Attacks
• DDos-Attacks on
– DNS
– Banks
– Energiy supplier
– Spamhaus
• Hacking/Malware
– Stuxnet
– Banks
– Saudi-Aramco
• Crtical attacks on governmental networks in DEU 2012 > 4.000


Cyber risk spectrum
Cyberwar
Cyberterrorism
Cybercrime (+ Espionage, Sabotage)
Hacktivism
Breach of compliance



„…cyberthreats constitute a new set of strategic threats that must be taken very seriously by states.“


Cyber Attacks are „currenttly the most dangerous threats.“
A. BLATTMANN,
Armeekommandant Schweiz


"Cyberwar, …
is the
most dramatic
of all potential
threats."
Joseph S. Nye
Harvard University

Klaus Naumann, ehemals Generalinspekteur der deutschen Bundeswehr und Vorsitzender des Militärausschusses der NATO. In: ÖMZ 2/2014, S. 142.

„…from Cyber Crime over Cyberterrorism … to Cyberwar ...

„…2020 big states …will be capable … to eliminate small states … electronical “…

Thesis for Cyberwar

- Highly developed countries depend on their infrastructure.
- Strategic infrastructure depends on the effective functioning of the information and communications technology.
- A sustained attack on the strategic infrastructure can lead to a policitical exploitable result.

Dependencies

Tabelle 2

Dependenzen der Teilsektoren

Ausfall des Teilsektors → / Auswirkung auf Teilsektor ↓	Stromversorgung	Telekommunikation	Informations-systeme und -netze
Stromversorgung	–	2	1
Telekommunikation	3	–	3
Informationssysteme und -netze	3	2	–
Internet	3	3	3
Instrumentations-, Automations- und Überwachungssysteme	3	3	3
Rundfunk und Medien	3	2	3
auf alle 31 Teilsektoren	68	45	45

Bewertet wurden auf einer vierstufigen Skala von 0 (keine Auswirkungen) bis 3 (sehr große Auswirkungen) – unter der Annahme eines Totalausfalls während dreier Wochen in der ganzen Schweiz – die Dependenzen der 31 Teilsektoren voneinander.
Quelle: BABS 2009, S. 10, Ausschnitt aus der dortigen Abbildung 4

Threat: A Scenario

- **Simultaneous attack on**
  - –Headquarters of electricity suppliers
  - –Main server of IT-companies
  - –Banks and money suppliers
  - –Austrian Army, Ministry of Interior Affairs
  - –Security Agencies and other authorities
  - –Root Server DNS of the www
  - –Air traffic control centres, airports
  - –Power plants and reservoir control
  - –National Railways, supply companies
  - –Food supply, water supply, sewage disposal
  - –Austrian Broadcasting Corporation, other media
  - –Hospitals, emergency facilities

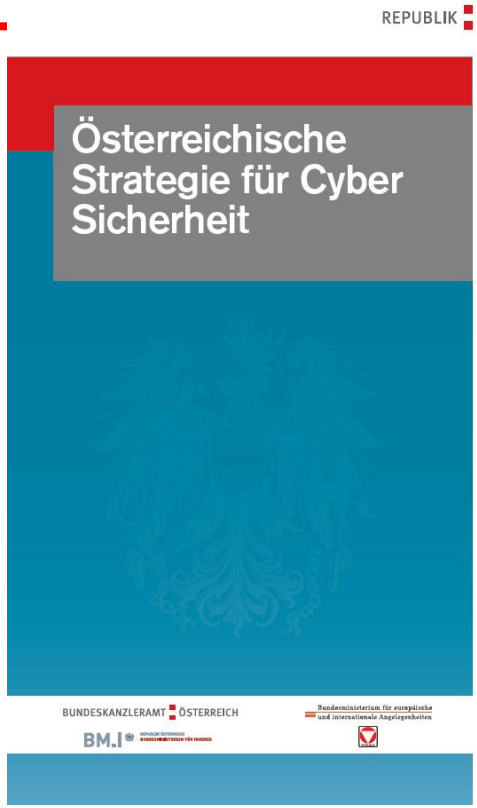
- **Ways & methods**
  - –Worms, virus and trojans
  - –Botnets
  - –Destruction of optical fibre cable
  - –Destruction of Telecommunication stations
  - –Fire in a data centre
- **Requirement of time: forward planning 18-24 months**
- **Financial need: € 10 Mio.**
- **Staff requirements:**
  - –Malware programmers
  - –Agents for Reconnaissance and Sabotage

Deduction & challenges

- Preparations activities are difficult to detect
- A widespread attack focused on the critical strategic infrastructure is possible
- Critical infrastructure is mainly in private ownership
- What kind of ressources are required?
- Active Defence
- Who is in charge?
- Attribution
- Redundant systems for the government activities and communications
- International cooperation

Cyber Attacks are a real threat!

We must be prepared!



https://www.bka.gv.at/DocView.axd?CobId=50999

BUNDESKANZLERAMT ÖSTERREICH

BM.I REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNERES

Bundesministerium für europäische und internationale Angelegenheiten

Cyber Resposibilities

BUNDESKANZLERAMT ÖSTERREICH

National Cyber Security

Fight against Cyber Crime

BM.I

Cyber Defence

Cyber Diplomacy

BMeiA

Cyber Security Private Sector

Cyber Security

Cyber Defence

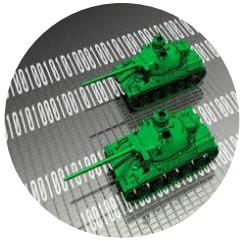
Mission AUT MOD
Cyber Space

Cyber Defence

CERT

Computer Emergency Readiness Team

Improve national cyber defence posture

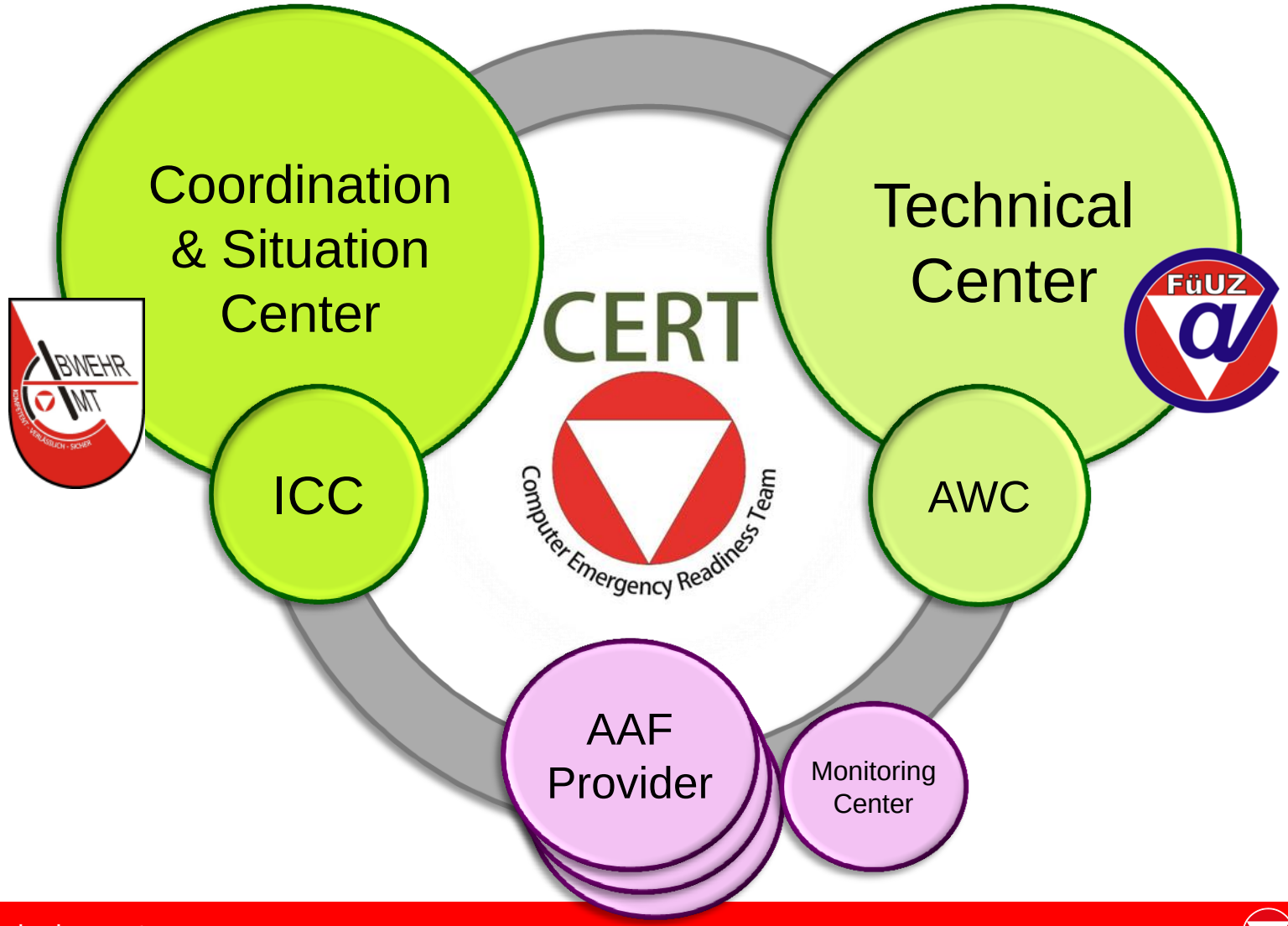


Support of military operations

Cyber common operating picture

Incident management

milCERT Cluster



Services
Computer Emergency Readiness Team

operated by:

Reactive

- response to incidents
- response to vulnerablities
- analysis of artefacts
- emergency recovery

Proactive

- cyber common operating picture
- alarm and warning services
- risk analysis
- information gathering
- national and international networking
- awareness

Knowledge Management

- knowledge management cyber defence
- provide a CyDef knowledge base
- support and improvement of all processes
- product evaluation

Way Forward

FOC 2015

IOC 2014