Estonian
Information System's
Authority

CYBER SECURITY TRENDS AND CHALLENGES

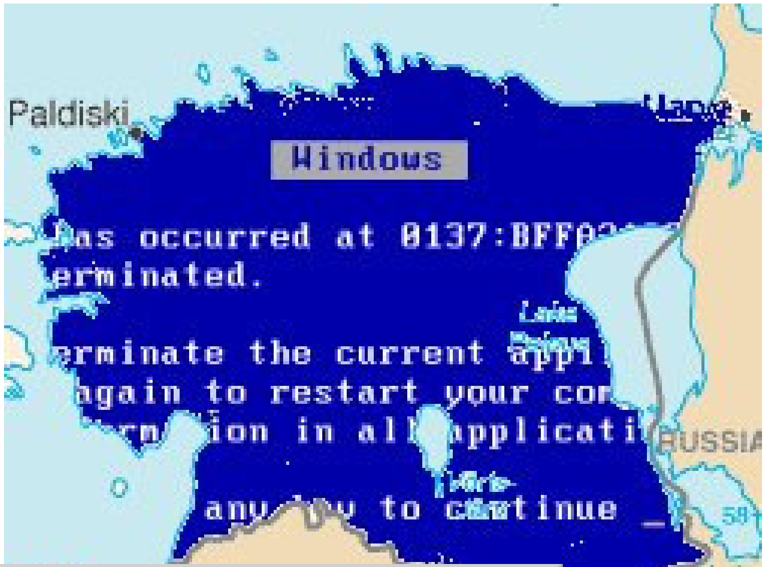
February 29, Riga

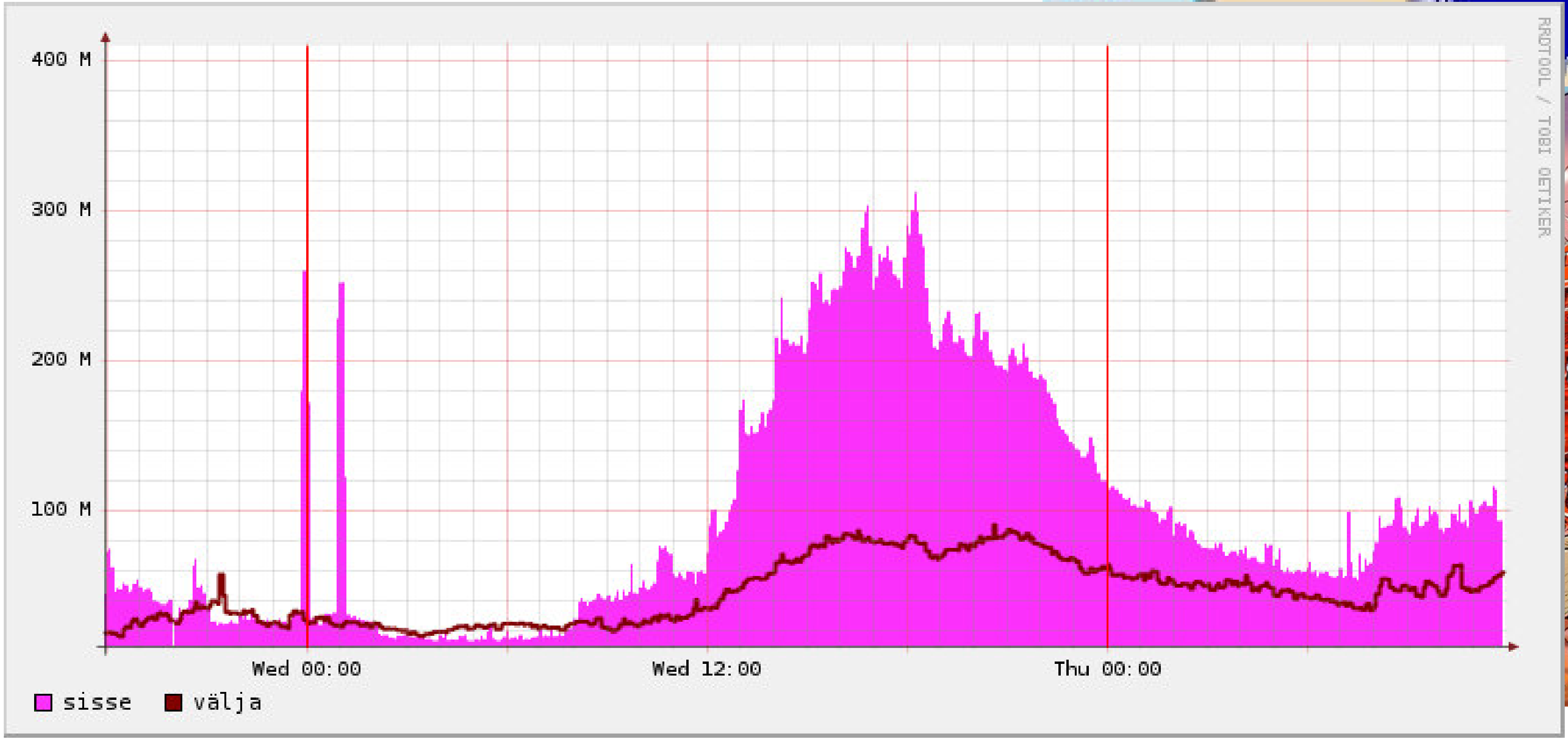
Presentation to LATO
Luukas Ilves
International cooperation, EISA, Tallinn

April 2007

April 2007

April 2007 in Cyberspace





ERNITS

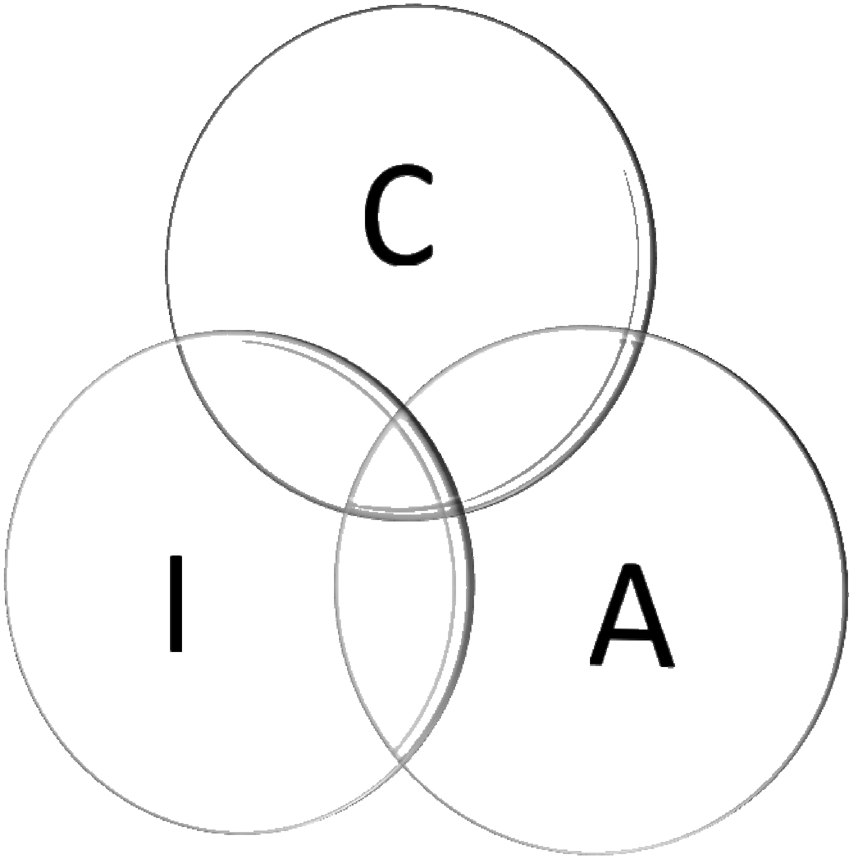
Defending an e-way of life

E-stonia – a balanced demand and supply of e-services from private and public sector

E-solutions widely in use and dependable

- 98% of banking
- 92% tax declarations
- M-parking
- Ca 1,148,000 national ID cards issued
- Sign and encrypt documents using E-ID
- E- & M-voting
- National Electronic Health Records
- Public transport ID-ticket, ID-fishing licenses etc etc

Types of attacks

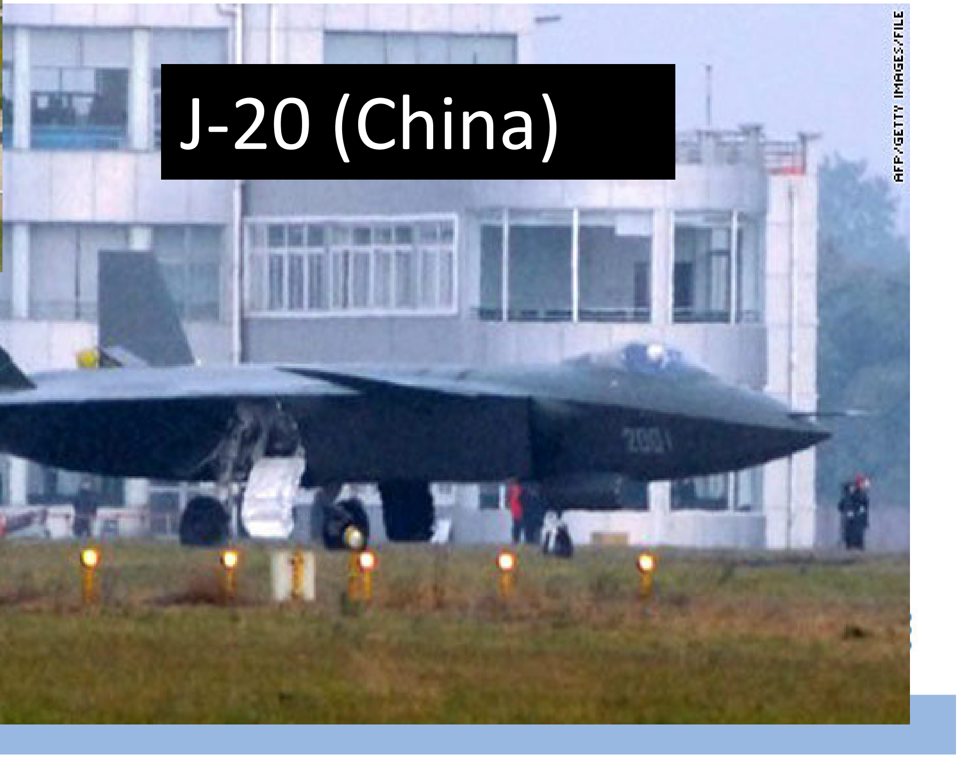


CONFIDENTIALITY

WikiLeaks
Have documents the world needs to see?
We help you safely get the truth out.
...ernments and inst

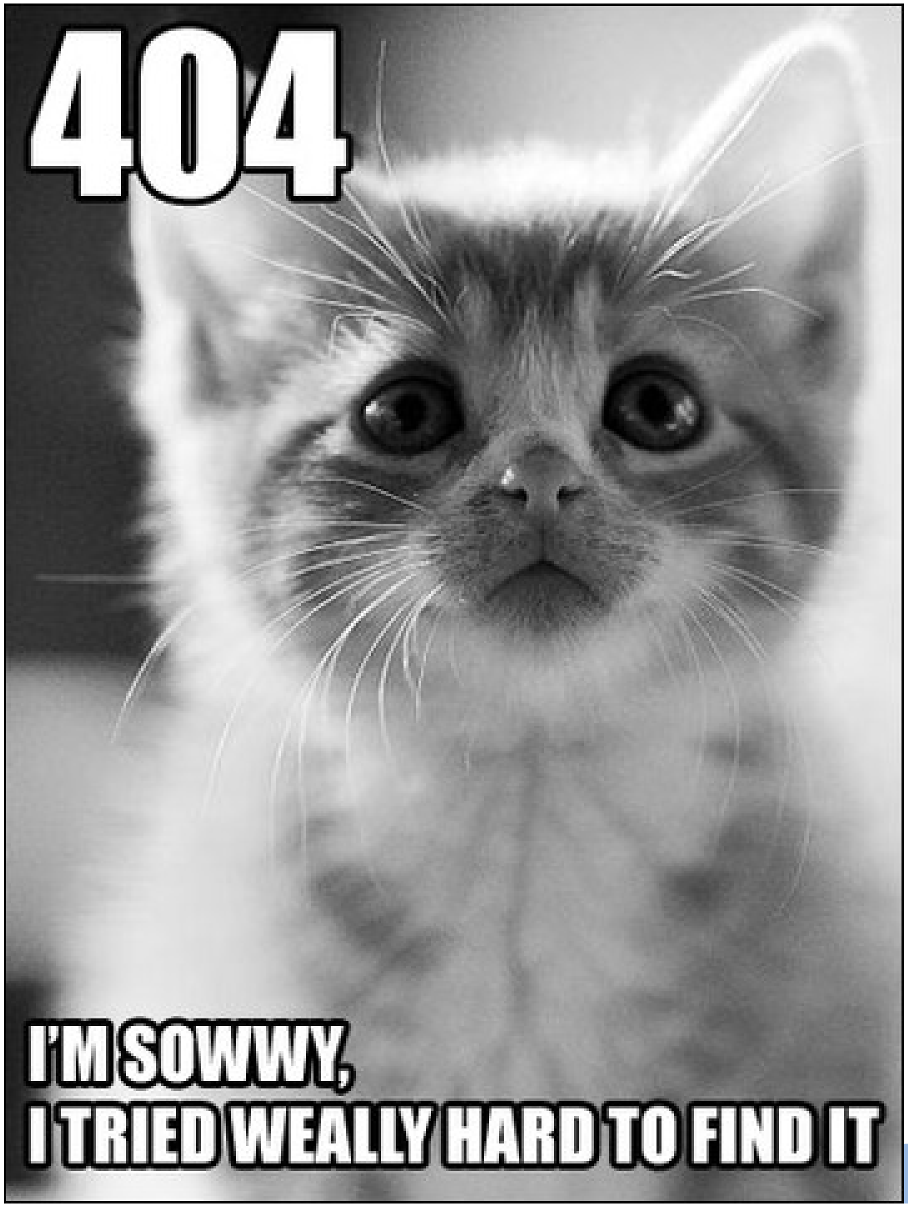
CONFIDENTIALITY

F-35 (US, Allies)


J-20 (China)

AFP/GETTY IMAGES/FILE

AVAILABILITY



INTEGRITY

Who are the bad guys?

(everybody)

Cyber criminals

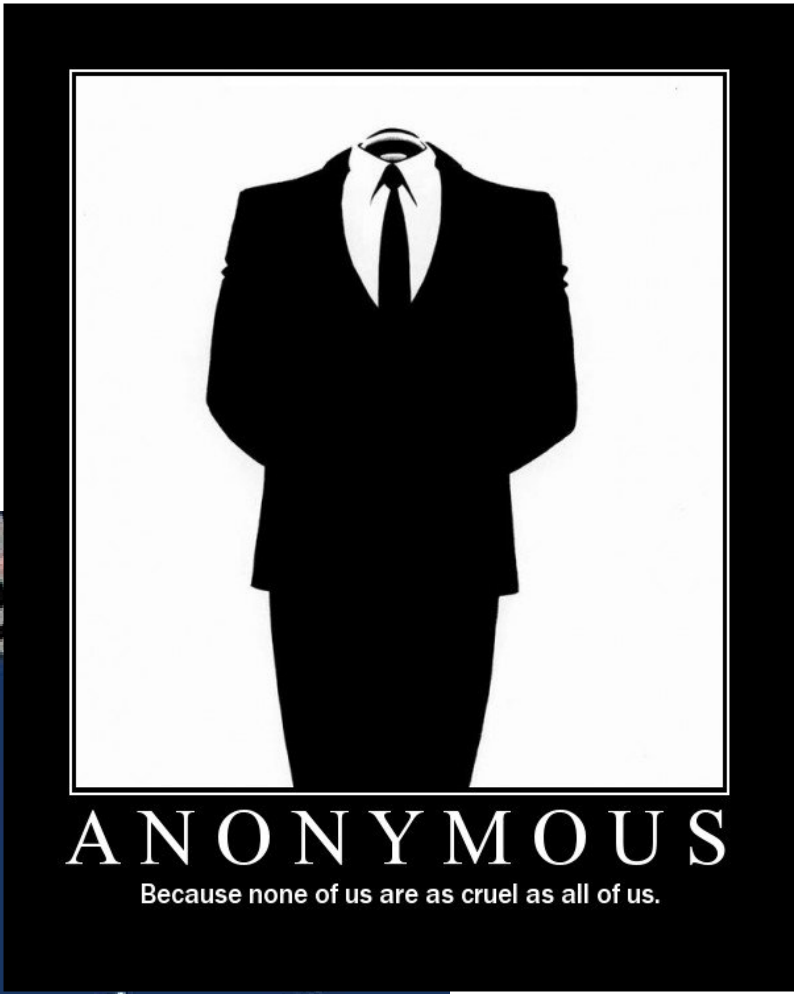
10 NOTORIOUS CYBER GANGS

1

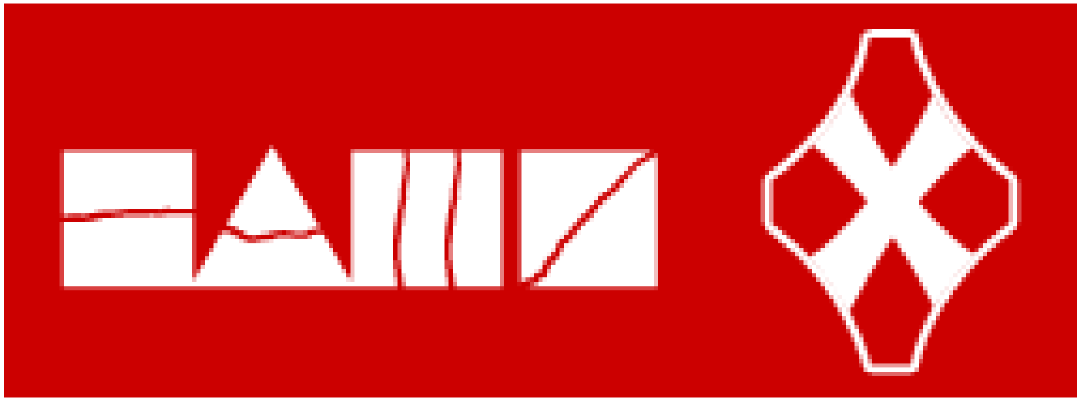
RUSSIAN BUSINESS NETWORK

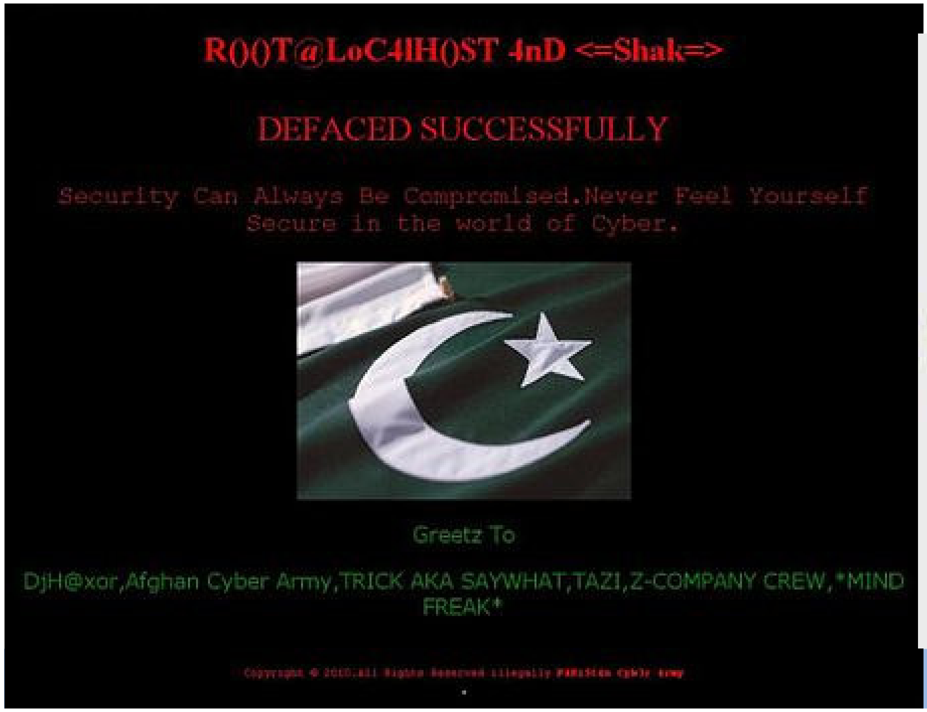
THIS NETWORK OF CRIMINALS WAS brought together in 2004 to provide hosting that would not take down cybercriminals' shady sites as long as they paid their bills. Today, researchers use the RBN moniker to label a number of the former RBN clients in order to conceptualize this dangerous group still up and running scams daily.

Hacktivists



Terrorists





R()()T@LoC4lH()ST 4nD <=Shak=>

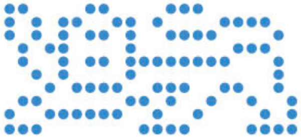
DEFACED SUCCESSFULLY

Security Can Always Be Compromised.Never Feel Yourself Secure in the world of Cyber.

Greetz To

DjH@xor,Afghan Cyber Army,TRICK AKA SAYWHAT,TAZI,Z-COMPANY CREW,*MIND FREAK*

Copyright © 2010.All Rights Reserved illegally PAKistan Cyber Army



States

Threat environment in cyberspace

- No clear dividing line between criminal or terrorist activity and strategic attack

- Cyber attack is low-cost, technologically available, asymmetric, crosses borders

- No attribution for attacks, many 3rd parties

- Civilian critical infrastructure and private sector most vulnerable

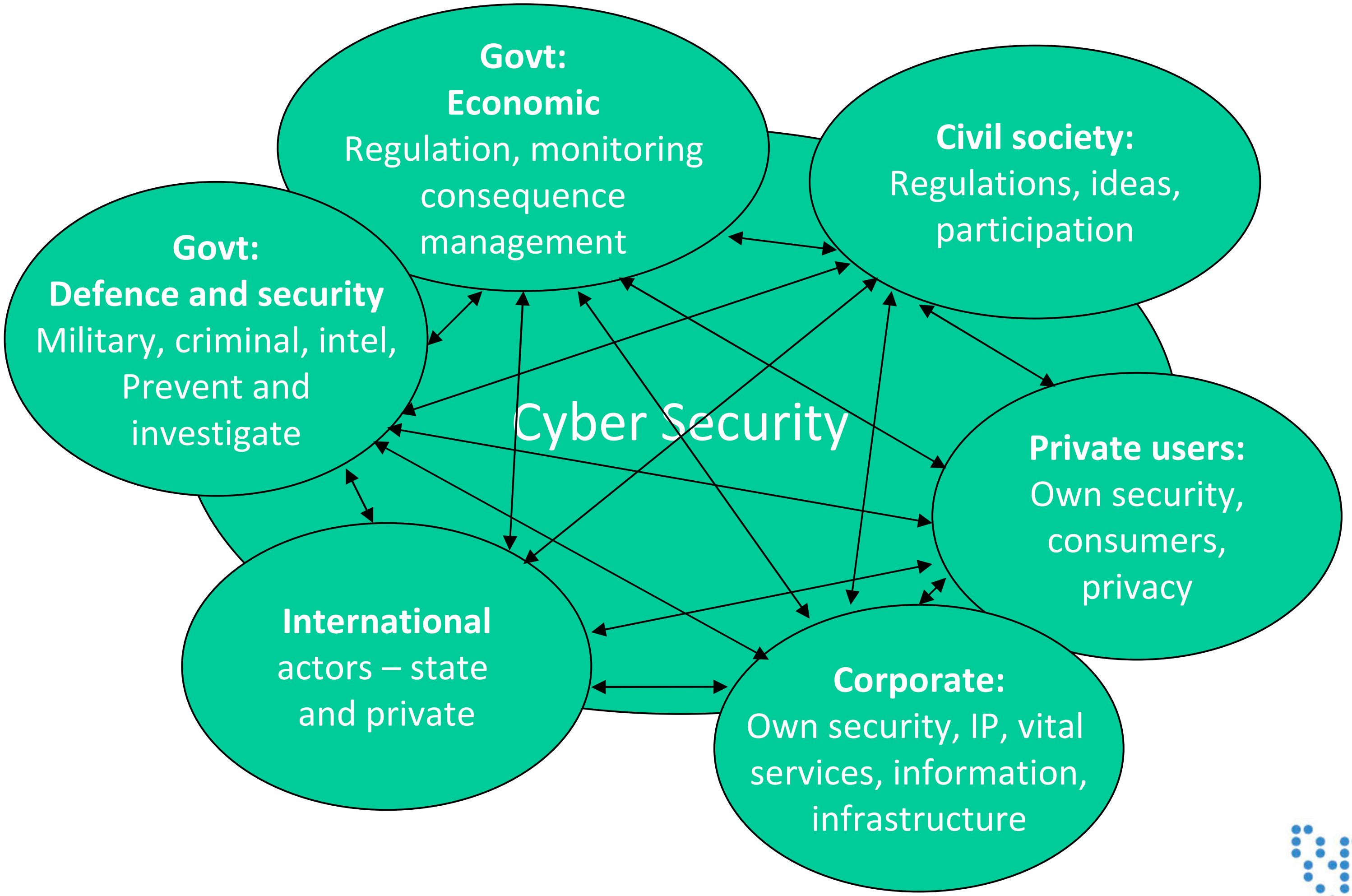
- Not a “new threat”, but “new vulnerability”

- Policy goal: extend rule of law and stability into a chaotic domain

So what to do?

Estonia’s approach to cybersecurity

Many responsibilities



Govt:
Economic
Regulation, monitoring consequence management

Civil society:
Regulations, ideas, participation

Govt:
Defence and security
Military, criminal, intel, Prevent and investigate

Cyber Security

Private users:
Own security, consumers, privacy

International
actors – state and private

Corporate:
Own security, IP, vital services, information, infrastructure

A whole-of-country approach

Legislation and regulations up to date

National Cybersecurity Council provides cabinet-level and inter-agency coordination

Public-private partnerships with private sector companies, civil society, individuals

Private-private partnerships

Create a **collective brain**

International strategy

Legislation

National Cyber Security Strategy of 2008

- Creation of a cabinet-level **National Cyber Security Council**
- Restructuring of the **Estonian Informatics Centre** for critical civilian information infrastructure protection and monitoring the country's cyber space

Emergency Act of 2009

- Cyber attacks can constitute a national emergency
- Re-definition of critical services and coordinating agencies in light of lessons learned
- Compulsory baseline IT security standards for the public sector
- Nation-wide early warning system
- Creation of the Cyber Defence League

National Level:
Estonia’s whole-of-country approach

Legislation and regulations up to date

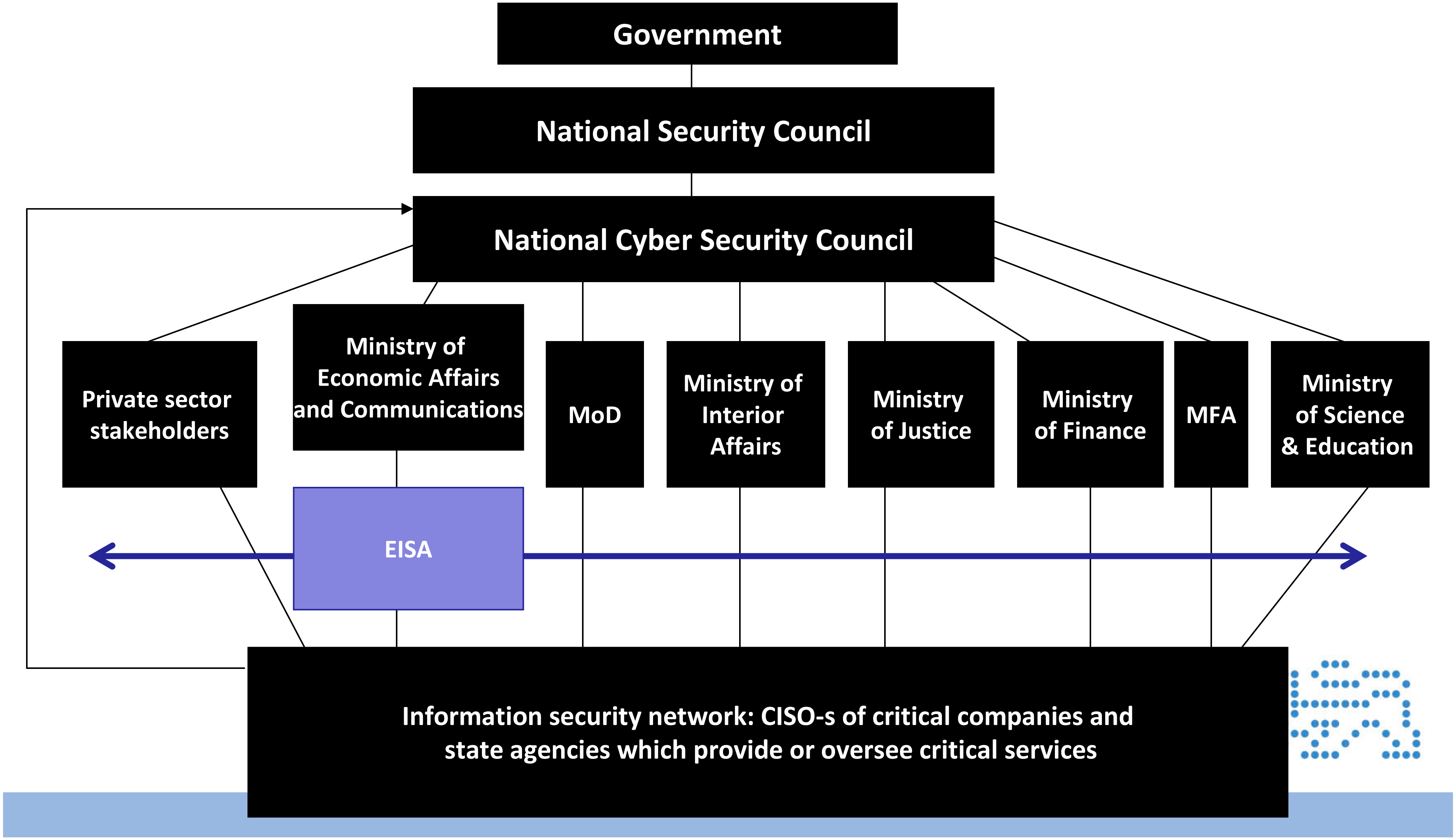
National Cybersecurity Council provides cabinet-level and inter-agency coordination

Public-private partnerships with private sector companies, civil society, individuals

Private-private partnerships

Contribute **internationally**

National organization



Government

National Security Council

National Cyber Security Council

Private sector stakeholders

Ministry of Economic Affairs and Communications

MoD

Ministry of Interior Affairs

Ministry of Justice

Ministry of Finance

MFA

Ministry of Science & Education

EISA

Information security network: CISO-s of critical companies and state agencies which provide or oversee critical services

Not just government

Banks, major telecoms, etc

- Maintain services for the state and users
- Coordinate with the government, each other

Individual citizens, awareness and education

- Graduate programs in information security and cyber defence
- IS modules in BA programs, training for specialists
- Increased funding for IS research
- Primary and secondary education include computer safety classes in curricula

Public-private partnership

Identification of critical services/critical information infrastructure

Building and maintaining a dialogue with critical service providers

Regular assessment of IT vulnerabilities and interdependencies between critical functions

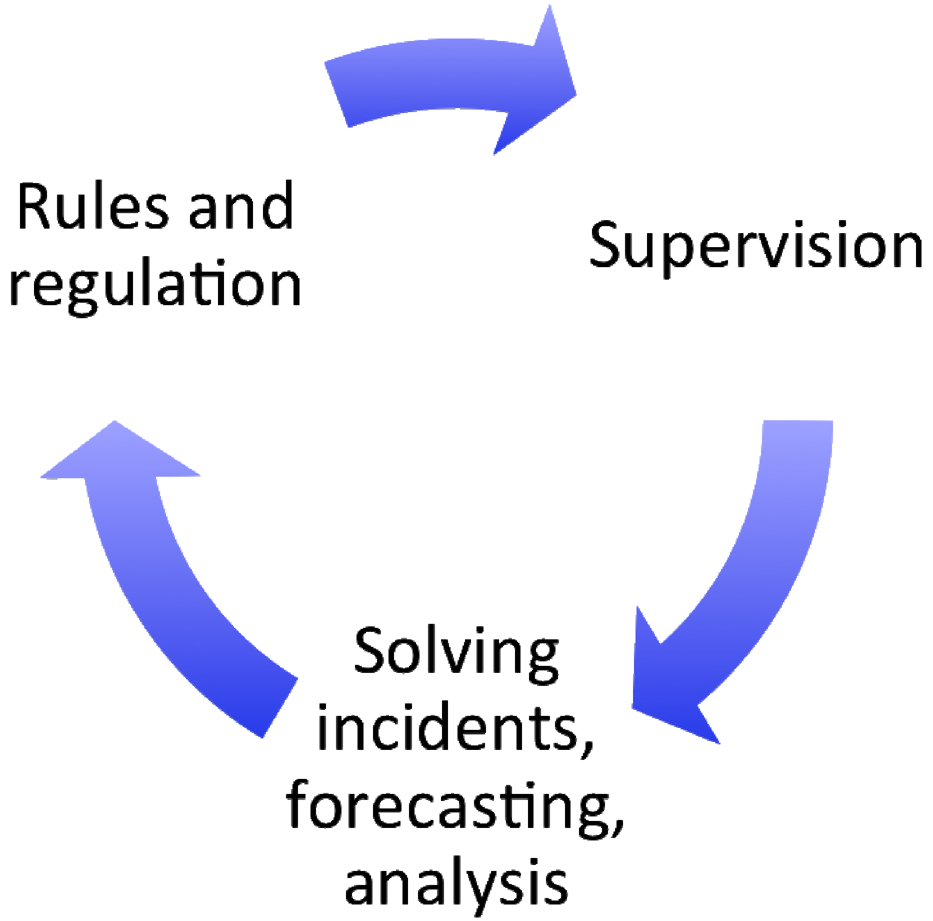
Maintaining a nation-wide early warning system with most critical companies

Furthering high level of infosec competence in society

Private-private partnership: Banks

EISA

- Since June 1st 2011, the Estonian Informatics Centre has been re-organised to the Estonian Information System's Authority (EISA).
- EISA develops national information systems (x-road, citizen portal) that provide e-government.
- The new authority helps private and public sector's organisations to maintain the security of their information systems, the authority has also the right of supervision.
- Re-organisation involves mostly two departments dealing with information security, and expands regulatory authority.



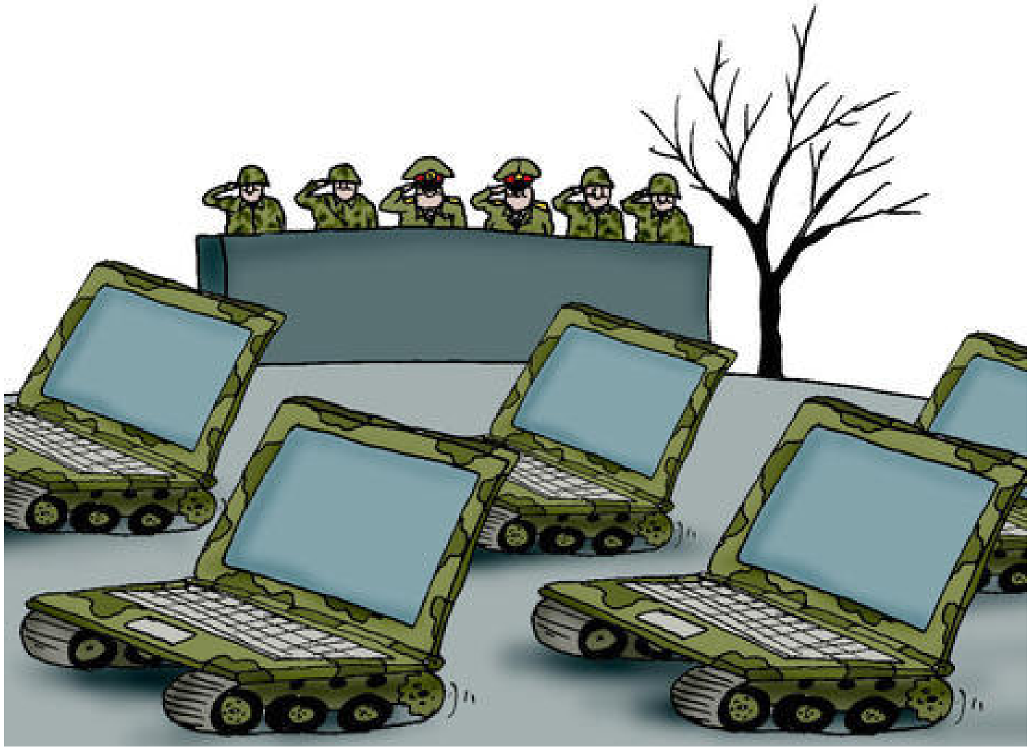
Rules and regulation

Supervision

Solving incidents, forecasting, analysis

Cyber Defence League

- A voluntary national cyber corps
- Both private and public sector experts
- Training, education and exercising in cyber security of national critical organisations
- Benefits the individuals, their employers as well as the country as a whole



NATO CCD CoE

- 10 nations (incl. Latvia)
- 3 focuses
    - Legal and Policy
    - Technical
    - Concepts and Strategy
- Conference
- Training courses

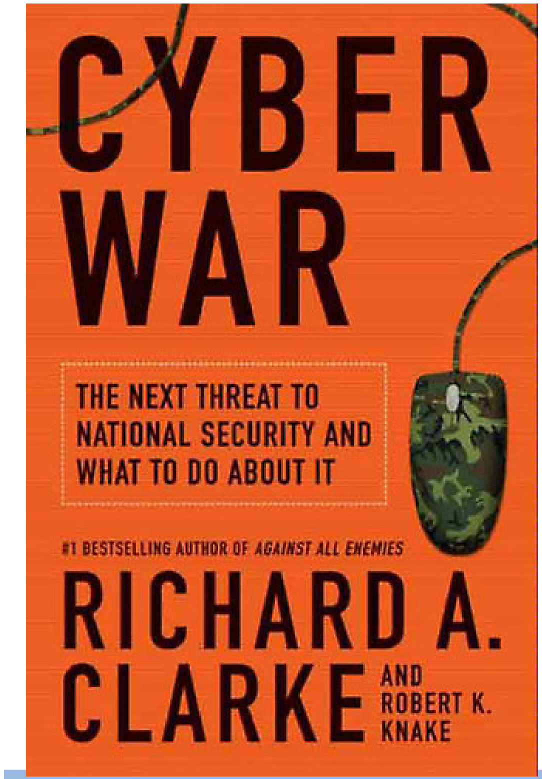
CCDCOE

Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

International

- Cyber-crime convention
- NATO
- EU
- CSDP/CFSP
- UN, OSCE
- B-3, NB-8

State of cyber in the US



CYBER WAR

THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT

#1 BESTSELLING AUTHOR OF *AGAINST ALL ENEMIES*

RICHARD A. CLARKE AND ROBERT K. KNAKE

European Union

Thank You!

Luukas Ilves

LUUKAS.ILVES@RIA.EE