REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Cyber emergency preparedness and response: Estonian approach

Lauri Luht
RIA Cyber Security branch

What I am going to talk about?

- Defending the “Cyber Environment”
- Myths
- Estonian environment for (cyber) emergency management
- Mostly about challenges… ☺

Terms

- Cyber defense/security
  - Defending the environment of the information society

- Information security
  - Data, comms, computers

Pick one! (T/F)

Emergency management is a complimentary and freestanding process

OR

Emergency management is part of everyday operations and functions

Background / Main principle

- How to be prepared and manage cyber crisis?
  (I am not talking about technical level)

- Forget about “cyber”…
- …and think about whole of security!

- Learn from working set-ups proven to be efficient over long years in other areas!

5 Myths of Cyber Security

- Cybersecurity Is Unlike Any Challenge We Have Faced
- Every Day We Face “Millions of Cyber Attacks”
- This Is a Technology Problem
- The Best (Cyber) Defense Is a Good (Cyber) Offense
- “Hackers” Are the Biggest Threat to the Internet Today

Peter W. Singer and Allan Friedman
(http://www.wired.com/2014/07/debunking-5-major-cyber-security-myths/)

What are we defending?

Layers of Defense

Country	→	Critical Infrastructure
Organisation	→	Process
Community	→	Culture
Person	→	Hygiene

Cyber defense is a total defense!

Against who we are defending?

- Criminals
- Hactivists
- Organised crime
- Terrorists
- State organised/financed crime
- Military

Cyber-attack

- Attack vs incident
- Cheap, achievable, crossing borders
- Thinking opponent
- Dependencies in private sector under attack
- Lack of right for state interference

Cyber-war is invisible!

Importance (why are we defending?)

- Cyber threats do not threaten only the virtual domain…
- …nor only those who deal with cyber…
- …they go kinetic!!!
- …and kinetic/physical threats may endanger life, health, well-being of humans

- For non believers ☺: https://www.youtube.com/watch?v=fJyWngDco3g

New approach (?)

- It's not about "computer emergency"!
  - Vulnerability of the society
  - Societal awareness – societal threat
- Cyber is part of all security
  - Uniqueness – time factor!
- Building legislation, organisational culture, rapid and dynamic risk management
- CERT vs SIRT (Security Incident Response Team)

The Future

- Growing complexity → challenges
- Growing dependency (& interdependencies)
- New “Pearl Harbour” will happen (K. Alexander)
- Isolation is expensive stagnation
- People are important
- The best collective brain wins

Basic principles and legislation in EE

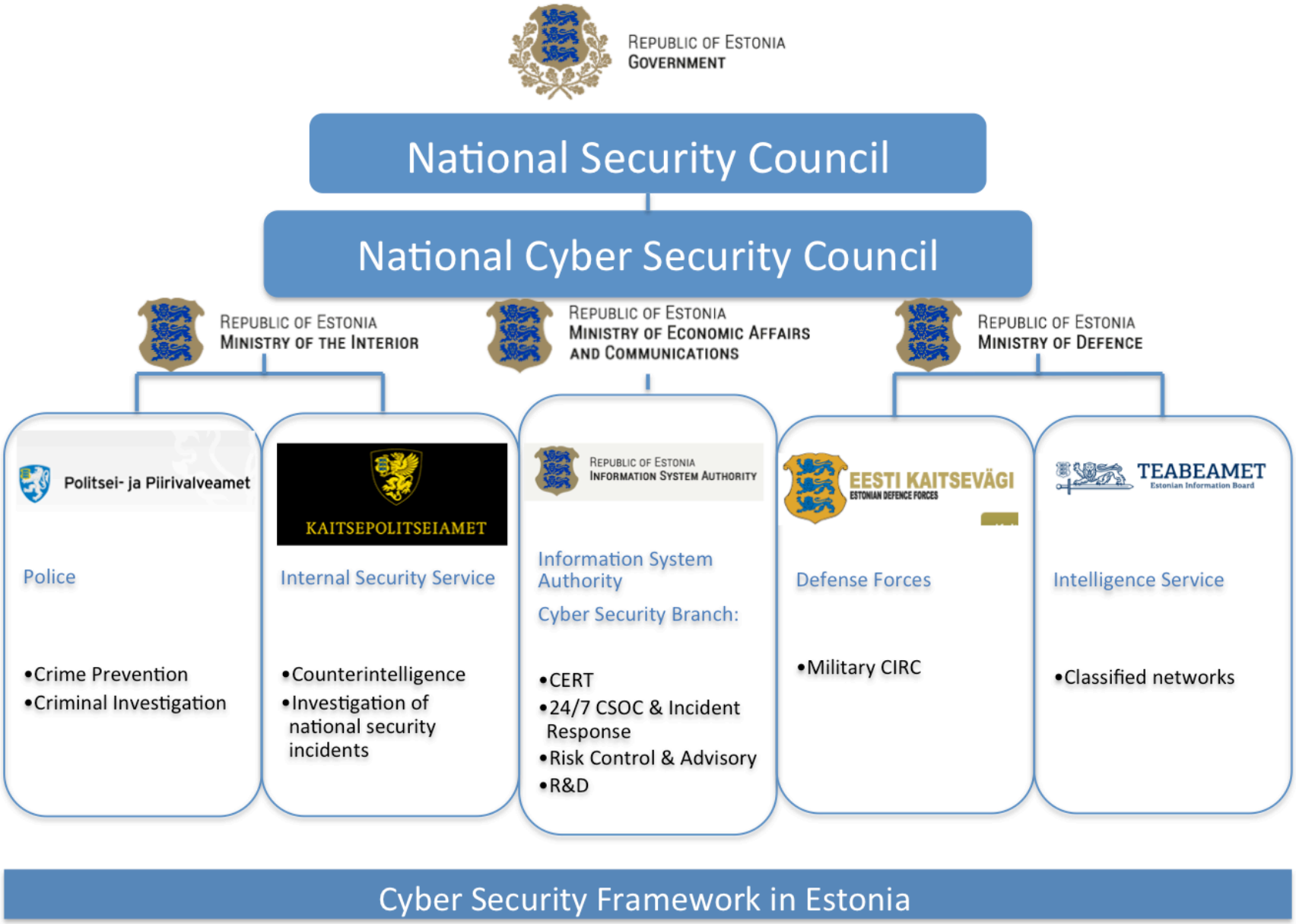
- Emergency Act (2009)
  - Decentralised system
  - Responsible authorities
  - Basing on co-ordination

- Emergency Response Plans (gov. orders)
- Protection of vital services: analysis and plans
- Security standards, stakeholder groups etc
- **NB! No specific law in cyber (field nor service)!**

Stakeholders in Cyber (in EE)

- RIA – **main coordinator – Responsible authority**
- Internal Security Service
- Information Board
- Police and Border Guard Board
- Defense Forces
- Cyber Defense Unit of the Defense League
- IT centers of ministries
- Prosecution
- Government office
- Ministries
- Vital services providers

…and many more...


Republic of Estonia
Government
National Security Council
National Cyber Security Council
Republic of Estonia
Ministry of the Interior
Republic of Estonia
Ministry of Economic Affairs and Communications
Republic of Estonia
Ministry of Defence
Politsei- ja Piirivalveamet
Police
•Crime Prevention
•Criminal Investigation
KAITSEPOLITSEIAMET
Internal Security Service
•Counterintelligence
•Investigation of national security incidents
Republic of Estonia
Information System Authority
Information System Authority
Cyber Security Branch:
•CERT
•24/7 CSOC & Incident Response
•Risk Control & Advisory
•R&D
EESTI KAITSEVÄGI
Estonian Defence Forces
Defense Forces
•Military CIRC
TEABEAMET
Estonian Information Board
Intelligence Service
•Classified networks
Cyber Security Framework in Estonia

National Cyber Emergency Response Plan

EE Cyber Emergency Response Plan

- Glossary
- Response levels
- Information gathering, analysis, exchange and situational awareness
- Operational planning and C&C organisation
- Communication (StratCom)
- International cooperation

Response levels (national)

- **I – Tactical/technical:** service provider/ organisation/ authority
- **II – Operational:** RIA operational staff (incl stakeholders upon necessity)
- **III – Strategical:** DG-s, heads of services, min. reps

- **IV – Political-strategic:** Government level

RIA's preparedness levels

- RIA's internal procedure for different threat situations
- Defined roles, obligations, tasks and their organisation between persons and teams
- Systematic approach for escalating and de-escalating
- Interoperability with other authorities
- Simplicity!

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Thank you!

Lauri Luht
lauri.luht@ria.ee