Estonian Cyber Security Strategy : A National Response in New Threat Environment

Markko Künnapu
Criminal Policy Department
Ministry of Justice of Estonia

Vulnerability and threat levels

- Global: global disruptions and chain-effects
- State level: attacks organised by states or state-sponsored actors against the functioning of the territorial states, conducted to support the conventional warfare or as a part of information operations
- Societal level: disruption of normal functioning of the society, possible casualties, caused by state-sponsored or non-state entities (e.g. terrorist groups)
- Sectoral level: attacks causing disruptions or malfunctioning of one or more vital economic sectors/critical infrastructure
- Industry level: attacks against a company or a group of companies causing significant economic losses
- Individual level: hostile activities towards the individuals in Internet, unprotected computers of home users

New paradigm in conflicts

What we have seen already?

- Large scale cyber attacks were organised with an attempt to destabilise a country highly dependent on ICT sector
- Cyber attacks were used as a part of a military conflict to disrupt communications of an adversary
- Regular intrusions to classified networks with an aim of espionage and as a demonstration of asymmetric power

Future?

- The likelihood is growing that there will be severe cyber catastrophies in future
- Malicious state-sponsored actors and terrorists exploit the most vulnerable part of cyberspace – civilian infrastructure

Asymmetry in cyberspace

- **Threat levels are interlinked in cyberspace. Every organisation or individual can be a target of a cyberattack:**
  - **Nation states**
  - **International organisations**
  - **Global corporations**
  - **Industries and groups of industries**
  - **Small businesses**
  - **Families and individuals**

- **Origin of the attacks : the networked actors of different sources and motivations (state or state-sponsored actors, organised crime, individual professionals, hackers, script-kiddies, hacktivists etc.)**

- **Response to the threat : hierarchies at several levels**

- **A result : response to cyber threats remains fragmented**

How to make policy responses working?

A new policy area waiting to be developed in a situation where:

- Information infrastructure is global, with very little gover**n**ance
- National capabilities and regulations are rather uneven
- There are a few informal, but very few institutional mechanisms for nation states for sharing information
- Private sector actors and individuals are at great risk sometimes
- Governments are looking for solutions mostly at national level, multinational cyber security efforts are still in embryonic stage

What we need to consider while designing policies?

- Cyber threats should not overshadow the positive aspects of using information technology and Internet
- Any efficient policy response should include private sector and individual citizens
- Involvement of all stakeholders is important

A need for comprehensive approach

NATIONAL LEVEL

- Including all professional communities, which will have their share in national cyber security effort
- Establishing an interagency coordination on cyber security
- Developing a national strategy and making sure all agencies and major stakeholders follow it
- Identifying a strong leading institution in national effort

INTERNATIONAL LEVEL

- Raising awareness beyond the industrial countries
- Strenghtening the efforts and launching new policies within the international organisations, establishment of permanent institutions for cyber security
- Working jointly on international cyber security initiatives to raise global awareness

International response

Policies:

- To share best practices on protecting critical information infrastructure
- To empower international incidence response and information sharing between national agencies
- To find international enforcement mechanisms for adopting minimal legal instruments on fighting cybercrime in third countries

Major existing international governmental policies and initiatives:

- EU CIIP policy based on a Commission Communication (30 March 2009)
- NATO Cyber Defence Policy and related initiatives
- EU information exchange network for critical infrastructure protection (CIWIN) and EU CIP initiative (EPCIP)
- Council of Europe Convention on Cybercrime
- OECD, G8 and other initiatives

Estonian Cyber Security Strategy

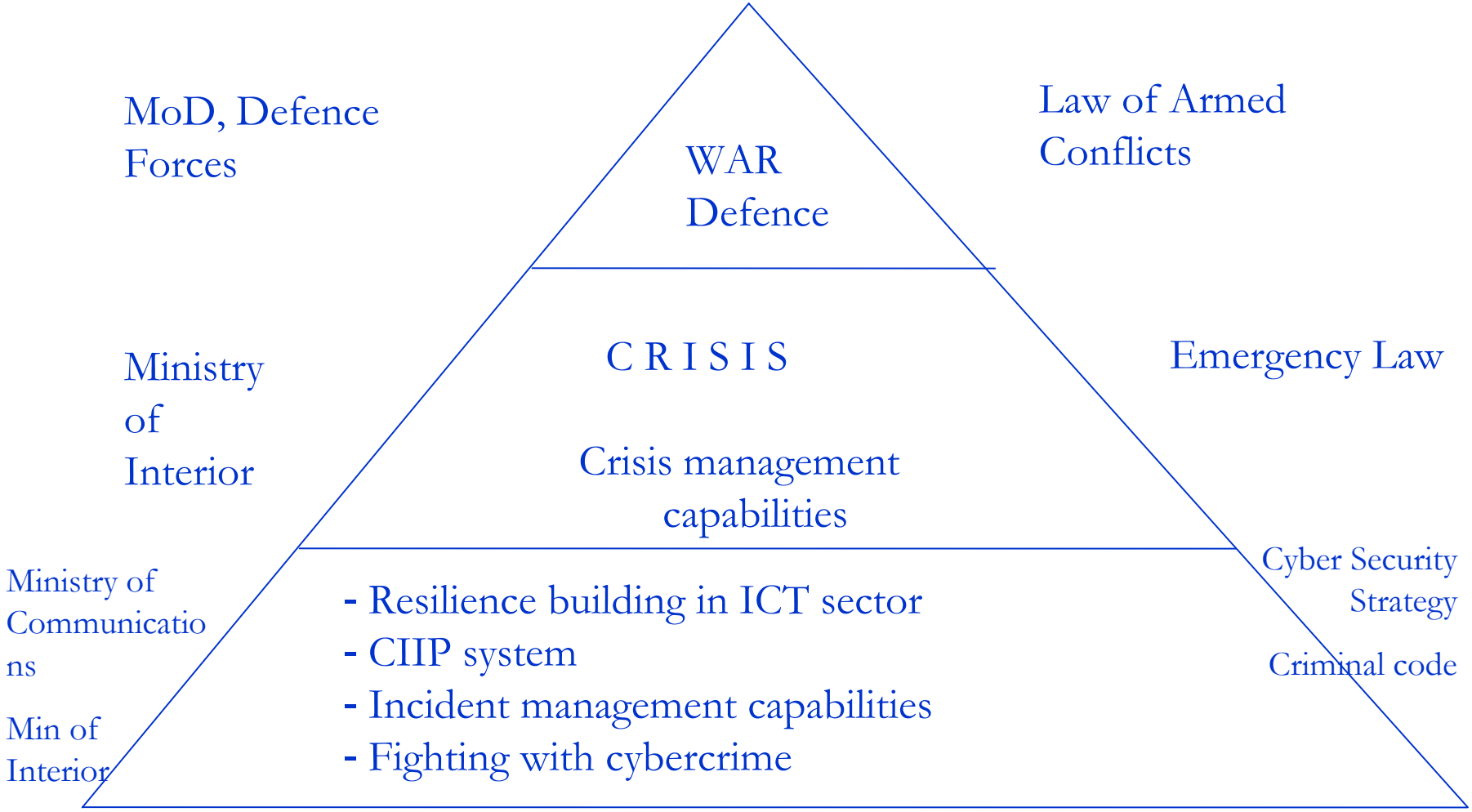
- To reduce vulnerability of country's cyberspace
- To enhance international cooperation, to promote cyber security culture and international initiatives
- To raise awareness on cyber security in whole society
- To advance the national system for protection of critical information systems and services
- To advance legal mechanisms that support the goals of the cyber security strategy

National policy development

A keyword : policy coordination

- **Setting clear national strategic goals**
- **Inclusion and cooperation: security analysts, technical experts, lawyers, diplomats, regulators**
- **Overcoming a gap between expert level and decision-makers**
- **Establishing and maintaining dialogue with private sector**
- **Escalation mechanism to the highest decision-making level**
- **Educating and briefing top decision-makers**
- **Institutional changes**

National capability pyramid



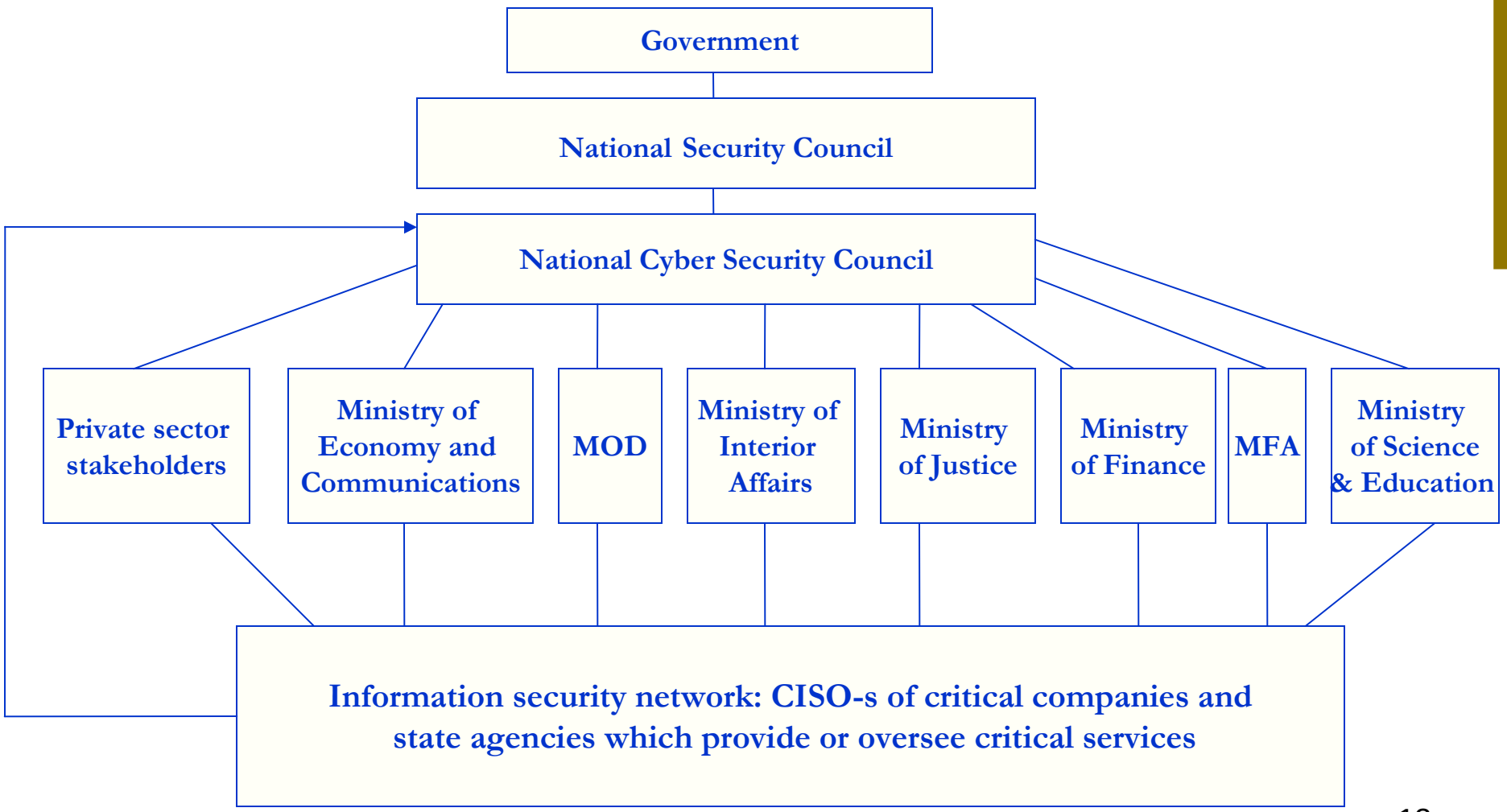
Protection of critical information infrastructure

- The Cyber Security Strategy introduces a system for nation's critical information infrastructure protection
- New methods of vulnerability assessments of CII, determining interdependence of CII,
- Implementation of additional security measures for critical information infrastructure
- Legal framework supporting this system
- Improvement of interdepartmental coordination, new structures for warning, advising and oversight of CII
- International measures of CIIP

CIIP system

- Determining dependence of critical services on IT services
- Mapping CII interdependence
- Annual vulnerability assessments
- Development of additional security measures (EMI-resilience, alternative basic infrastructure)
- Attention to SCADA systems
- Strengthening Internet infrastructure
- Increasing incident management capability
- Improving forensics capabilities
- Organisational measures to guarantee implementation of the strategy

Organisational chart



Awareness and training programs

- **Priority target groups - home users, small and medium businesses, system administrators**
- **Launching the targeted campaigns, social marketing, special programs**
- **Training programs for non-CII system administrators**
- **Private-public initiative “Defend your computer”**
- **Ppromotion of advanced end-user security measures (electronic signatures, authentication by ID cards)**
- **Courses for public and private sector executives**

Education and R&D

- New graduate programs in information security and cyber defence
- IS moduls included to all IT programs at the BA level
- IS training and non-degree courses for specialists
- Increased funding to information security related research
- Primary and secondary school curriculas have a computer safety classes within technology module
- Educating young generation and introducing cyber culture is the best investment for the future

Thank you!