Strategic Cyber Security Objectives and Implementation

[Event]

Kadri Kaska
NATO CCDCOE
27 November 2015

Outline

- National approaches to cyber security: national cyber security strategies and organisation
- International law applicable to cyberspace?
  - Territorial Sovereignty and integrity in cyberspace
- State responses to cyber attacks under international law
  - Peacetime
    - Countermeasures and sanctions
  - Armed conflict
    - Law of Armed Conflict in cyber
- Tallinn Manual

Converging Dependencies

- **World**
  - Population — 7.3 billion
  - Internet population — 3.2 billion *(40% of population)*
  - Connected devices — ≈12.5 billion
- **European Union**
  - eGovernance — 49% of citizens, 88% of enterprises
  - eCommerce — 9-20% of enterprise turnover

Sources: The World Bank, Cisco IBSG, Eurostat

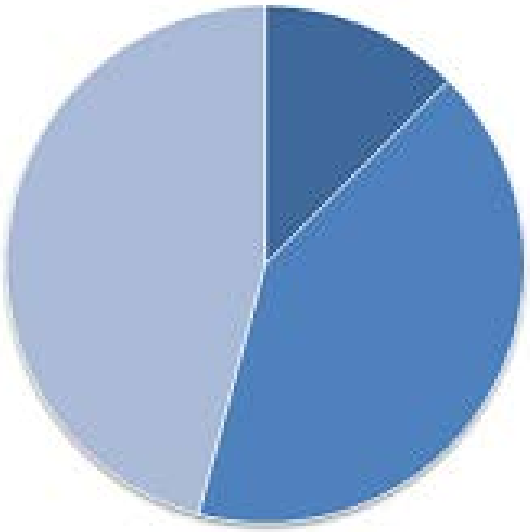
'Cyber just means interconnected ICT – but that increasingly means everything'

Cost of Connectivity

- Dependence of society on functioning information systems and communications networks
  - Vital services: 95% depending, 30% critical, 10% no low-tech backup
- Sources and nature of threats
  - Passive threats: natural and technological causes
  - Active threats: intentional activities
  - Various actors and motives

Strategic responses

NATO Nations
with a NCSS (2015)



PRE-2010 (3)
2010-2012 (10)
2013-2015 (11)

2nd Generation: 2014-2015 (4)

- NCSS inventory http://ccdcoe.org/strategies-policies.html
- 76 nations
  - 24 NATO
  - 22 EU (+2 EEA)
  - All world regions
- 140+ cyber security strategy and legal documents
- Periodically updated

National CS dimensions

- **Governmental**
  - Coordination between government actors
  - 'Whole of Government'
- **National**
  - Cooperation between state and non-state actors (academia, ICT providers, private individuals, NGOs)
  - 'Whole of Nation'
- **International**
  - International, transborder, 'like-for-like' collaboration
  - 'Whole of System'

Strategic objectives and priorities

Security of vital information systems

Combating cyber crime

Other (economic aspects; national defence)

Management structures and responsibilities

Coordination and cooperation

Awareness and competence

Core principles

Respect for fundamental values

Economic and social prosperity

Adequacy, effectiveness, proportionality

Five Dilemmas

Stimulate economy
vs. improve national security

Infrastructure modernisation
vs. critical infrastructure protection

Private sector *vs.* public sector

Data protection
vs. information sharing

Freedom of expression
vs. political stability

National Cyber Security Organisation

- Strategic CS leadership and cyber policy coordination
- Incident response and coordination
- Military cyber defence capabilities
- Cyber aspects of crisis management
- Cyber intelligence, private-public cooperation, etc.

https://ccdcoe.org/national-cyber-security-organisation.html

CONTACT

Kadri Kaska

kadri.kaska@ccdcoe.org

Filtri tee 12, 10132 Tallinn, Estonia +372 717 6800