Finnish Cyber Security Strategy

Permanent Secretary, LTG Arto Räty
Chairman of the Security Committee
15.1.2015, Geneva
Changing threat landscape

- Natural resources
- Interdependence
- Climate change
- Population growth
- Terrorism
- Global economy
- Technology
- Non-governmental actors
Annual losses caused by cybercrime over $400 billion (McAfee)

Cyber espionage on the rise (McAfee, Verizon)

Governments as the most important target (Symantec)
Finland cannot be a successful and competitive welfare state without a safe cyber domain
Comprehensive approach
Principles of Crisis Management

- President of the Republic
- Parliament
- Government
- Government-level preparation
- Interministerial Cooperation Bodies
- Ministry
- COMPETENT AUTHORITY
  Administration at central, regional and local levels
- Supporting authorities, business life and civic organisations
- National and international actors

www.turvallisuuskomitea.fi
Tasks of the Security Committee

To contribute to the preparedness of comprehensive security and its coordination

To monitor and evaluate Finland's security and defence policy environment and societal changes and their impacts on comprehensive security arrangements

To monitor the activities of different administrative sectors and levels to maintain and develop comprehensive security arrangements

To coordinate, if necessary, large and significant preparedness-related issues, such as national coordination of preparedness, development of forms of cooperation, operational models, research and training
Cyber Security Strategy Vision

VISION

Finland can secure its vital functions against cyber threats in all situations.

Citizens, the authorities and businesses can effectively utilise a safe cyber world and the competence arising from cyber security measures, both nationally and internationally.

By 2016, Finland will be the global forerunner in cyber threat preparedness and in managing the disturbances caused by these threats.
10 Cyber Security Guidelines

1. Collaboration model
2. Situational awareness
3. Continuity of preparedness
4. Capacities of the police
5. Cyber defence
6. Enhanced international co-operation
7. Education and training = knowledge
8. Legislation
9. Tasks, requirements and service models
10. Monitoring the implementation
Roadmap

**Strategy**
- Vision
- Strategic guidelines

**Memorandum**
- Securing the vital functions

**Implementation plan**
- Action items
- Cyber security tasks

**Implementation**
- Plans of the ministries

The strategy is a living document!
Implementation program

Main focus areas

- Cyber Security Center
- 24/7 Information Security Operations of the Government
- Security network for encrypted data transfer and administration
- Police’s responding capabilities to cybercrime
- Research and education programs, and improvement of other competences
- Changes in legislation
  - and if development of capabilities
Major Challenges

- Resources
- Full implementation of the National Security Network
- Roll-out of Government 24/7 Information Security Operations
- Legislation
- Responsibilities and coordination in some areas
- Some organisations are lagging behind in their implementation of the Information Society Code (earlier Information Security Law)
Implementation - where have we succeeded?

- Cyber Security Strategy and the implementation plan
- Cyber Security Center and development of the CERT
- Research, training and education programmes
- Innovation Centre in Jyväskylä
- Business Cyber Cluster (FISC)
- Working group on intelligence gathering - Report 14 Jan 2015
- Improved incident response procedures
- Cooperation between different actors
- Public-Private-Partnership
- International cooperation
- General knowledge and awareness
NCSC-Fi's role

Non-technical threats: Scams, frauds etc.

Technical threats

Actions ISPs take

General threats

APT

HAVARO

Unknown threats

End user controls

Citizens

Government

CIP

19.1.2015

www.turvallisuuskomitea.fi
First line – ISPs

Technical threats

Actions ISPs take

General threats

APT

HAVARO

Unknown threats

End user controls

Citizens

Government

CIP

Malware, DDOS, APT...

Communications market act, cleaning and disconnecting infected computers

Non-technical threats: Scams, frauds etc.
Result

Technical threats

Actions ISPs take

“Cleanest networks in the world”

General threats

APT

HAVARO

Unknown threats

End user controls

Based on Microsoft Security Intelligence Report 16

Non-technical threats: Scams, frauds etc.
Second line – HAVARO

Technical threats

Actions ISPs take

"Cleanest networks in the world"

General threats

APT

HAVARO

Unknown threats

Network Monitoring and Early Warning System

End user controls

Citizens

Government

CIP
Third line

Technical threats

Actions ISPs take

"Cleanest networks in the world"

General threats

APT

HAVARO

Unknown threats

End user controls

Citizens

Government

CIP

Every stakeholder is a security actor!
Finnish success factors

- Comprehensive concept
- Co-operation among authorities, businesses, and NGO’s
  - possibility to utilize existing knowledge and capabilities in Finland
    ➢ Cost-effectiveness!
- Shared awareness on the importance of cyber security
- Technology skills and knowledge
Security Committee
Eteläinen Makasiinikatu 8
P.O. Box 31, FI-00131 HELSINKI
Tel: +358 295 16001
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi