REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Digital Society: Opportunities and Challenges

Sven Kivvistik

Head of Risk Control & Advisory department, Cyber Security Branch
Estonian Information System Authority

15.01.2015
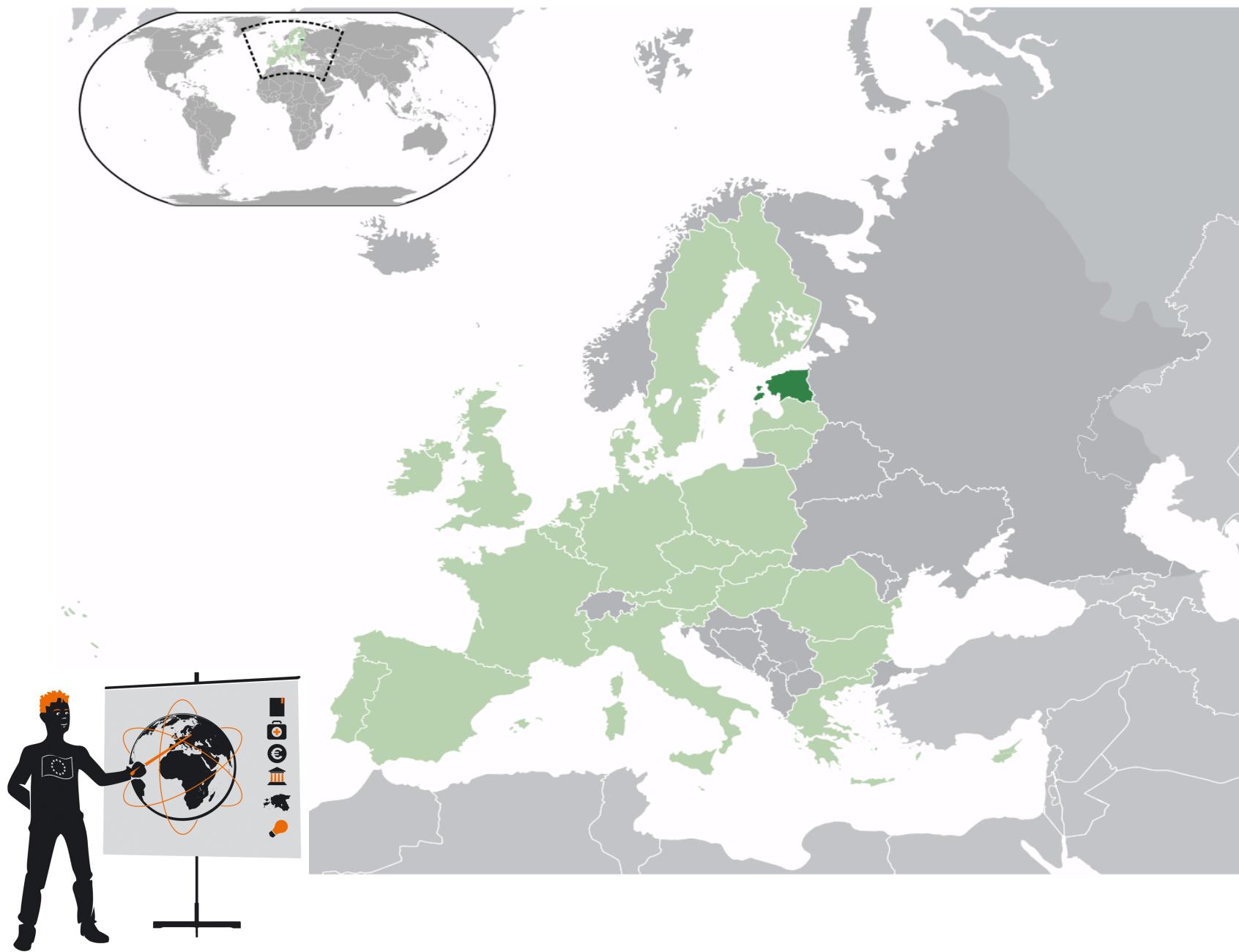
RIA – Estonian Information System Authority

The **Estonian Information System Authority** has 12 main duties, divided broadly into three area (https://www.ria.ee/about-estonian-information-system-authority/) :

- Development and administration of central e-government systems
- Overseeing of distribution of public funds for IT development
- Coordination of national cyber security
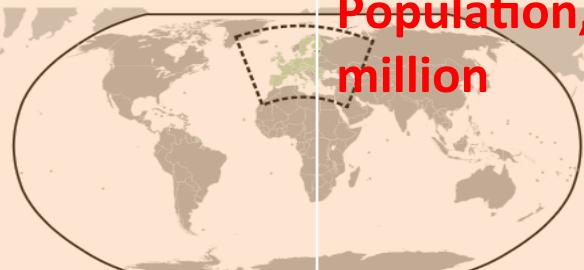
	Population, million	Territory Sin sq km thousand	Population density people per sq.km	GDP (PPP) per capita (EUR)
Estonia	1	45	31	19,675
Latvia	2	64	33	17,125
Russian Federation	140	17,098	9	16,602
Finland	5	338	17,8	30,848
Sweden	10	450	23,4	34641
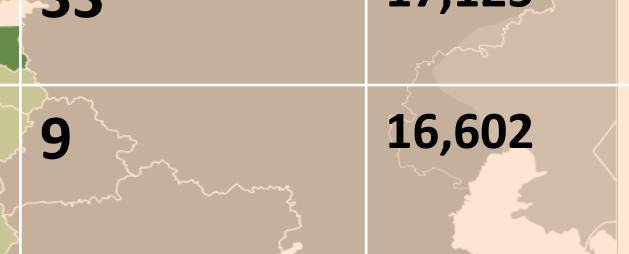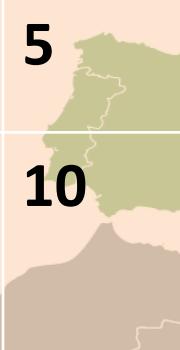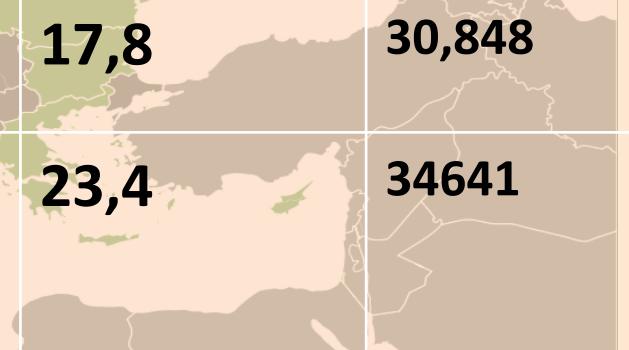
690 391

Baltic sea connections and interdependencies
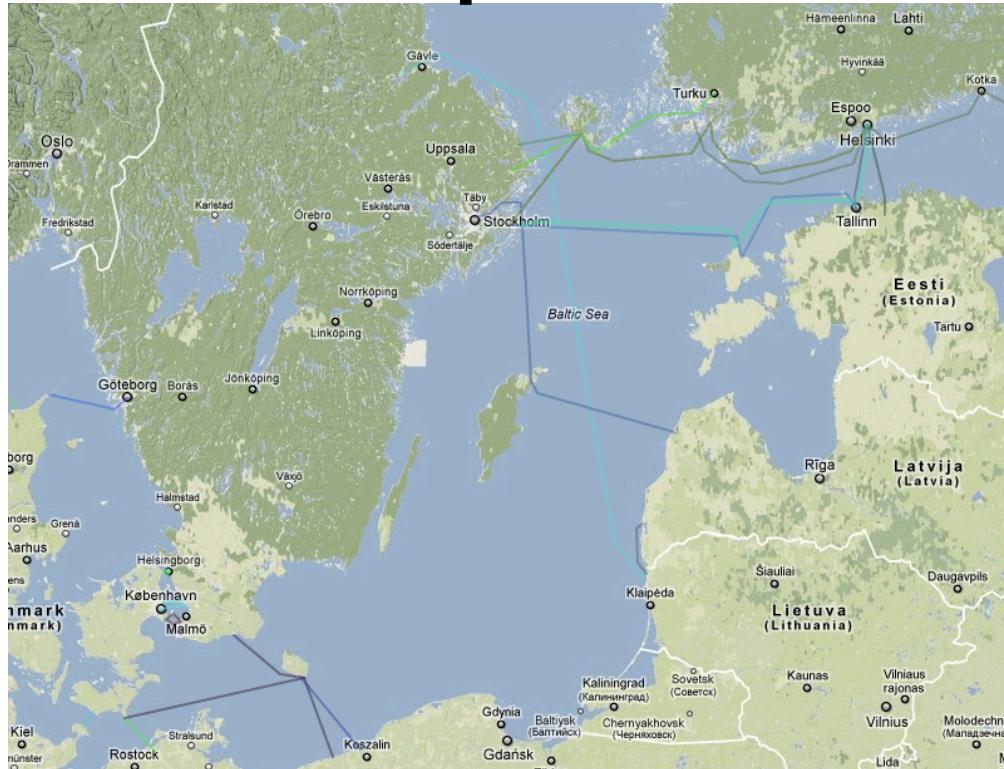
Weakest link
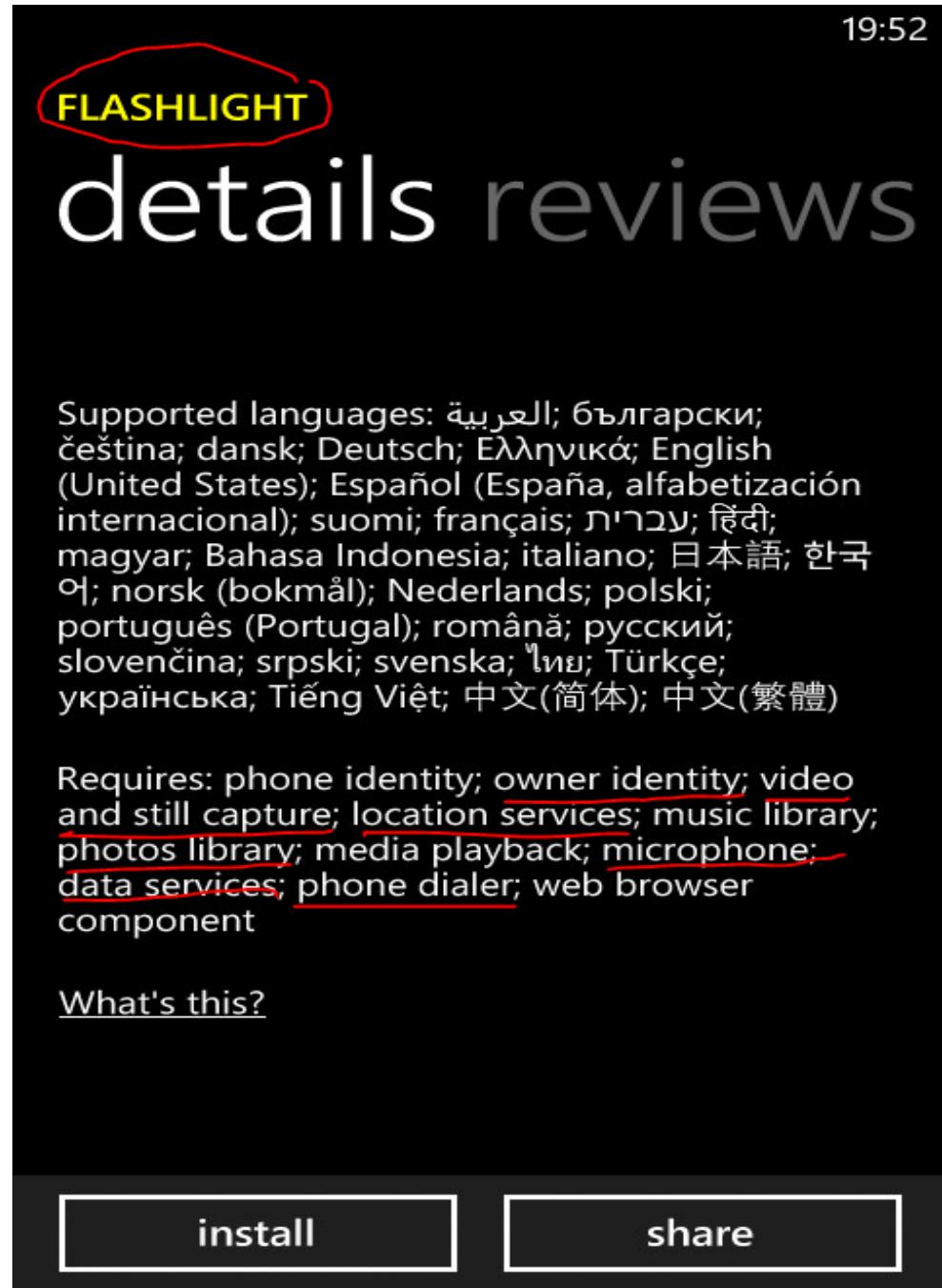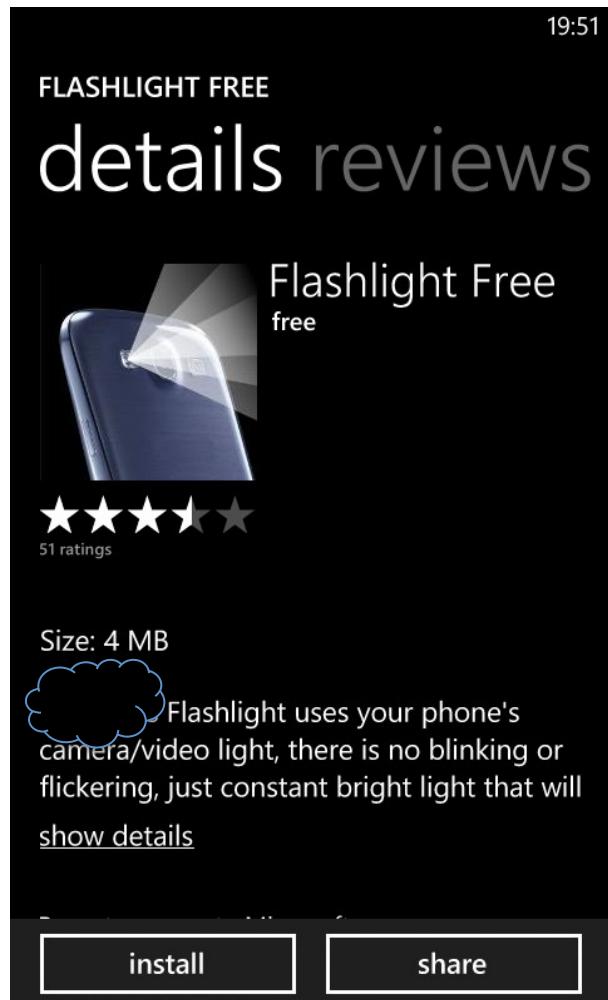
DNS Malware: Is Your Computer Infected?

DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse web sites, send e-mail, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.

- *Estonian authorities arrested six men, including **Vladimir Tsastsin**, 31, the owner of several Internet companies that have been closely associated with the malware community for many years. Tsastsin previously headed **EstDomains Inc**. a domain name registrar that handled the registrations for tens of thousands of domains associated with the far-flung Russian Business Network.*

Source: FBI

Against who we are defending?

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

Automated government
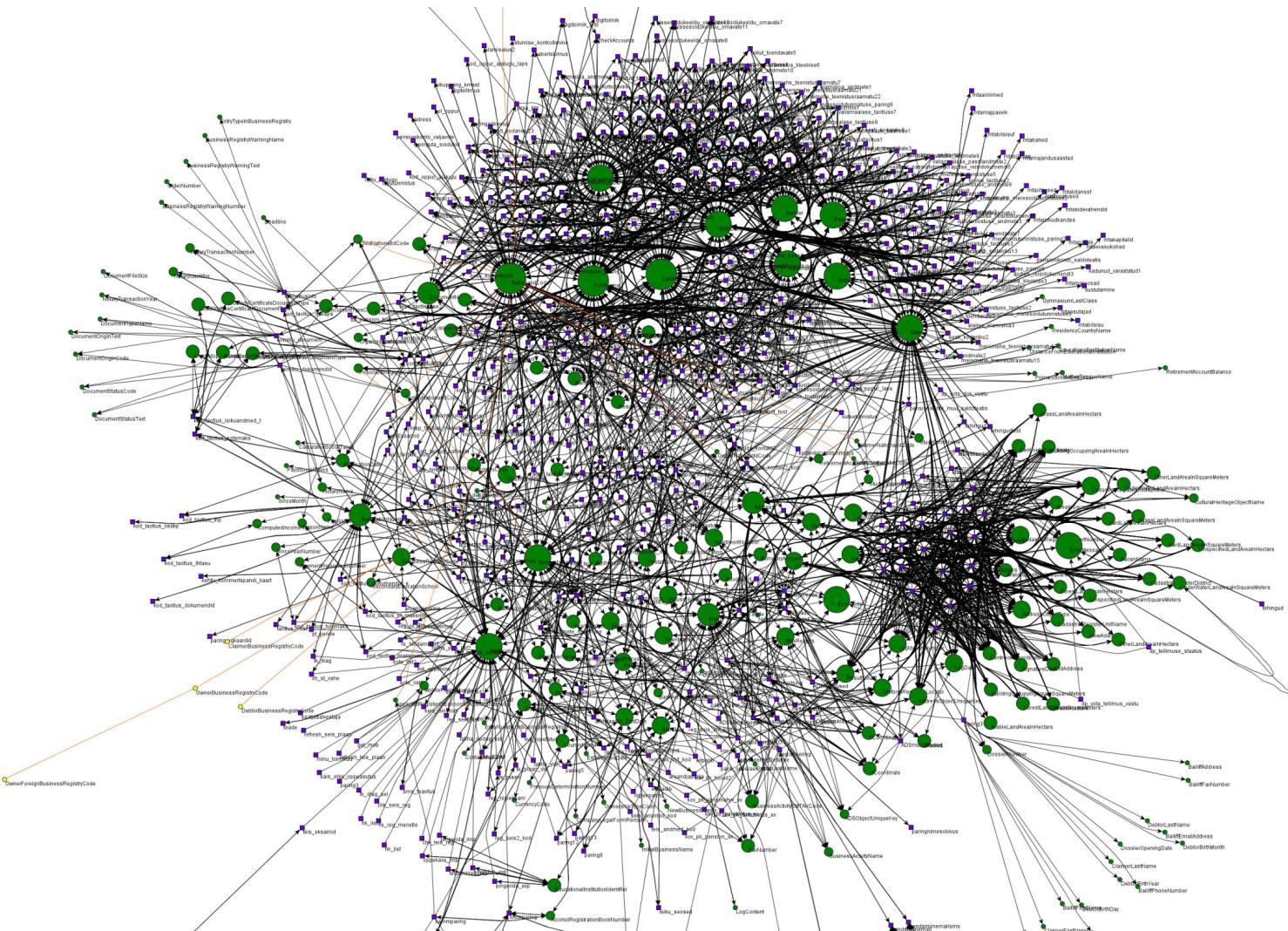
WHAT, HOW , WHO ?

Context

- **Population: 1,3M /Active eID: 1,2M**
  - one unique identifier for all public interactions
- **Data exchange** of information systems – **X-Road**
  - 1000 members connected, 3000 (1300) services
- State Portal **eesti.ee**,
- **I-voting** since 2005
- **'Once only' principle** – data re-use
- Very high penetration rate of public and private e-services,
- **Digital signatures: 44M / year**
  - Saving time: 1 week per capita

The Estonian State Portal in 2013
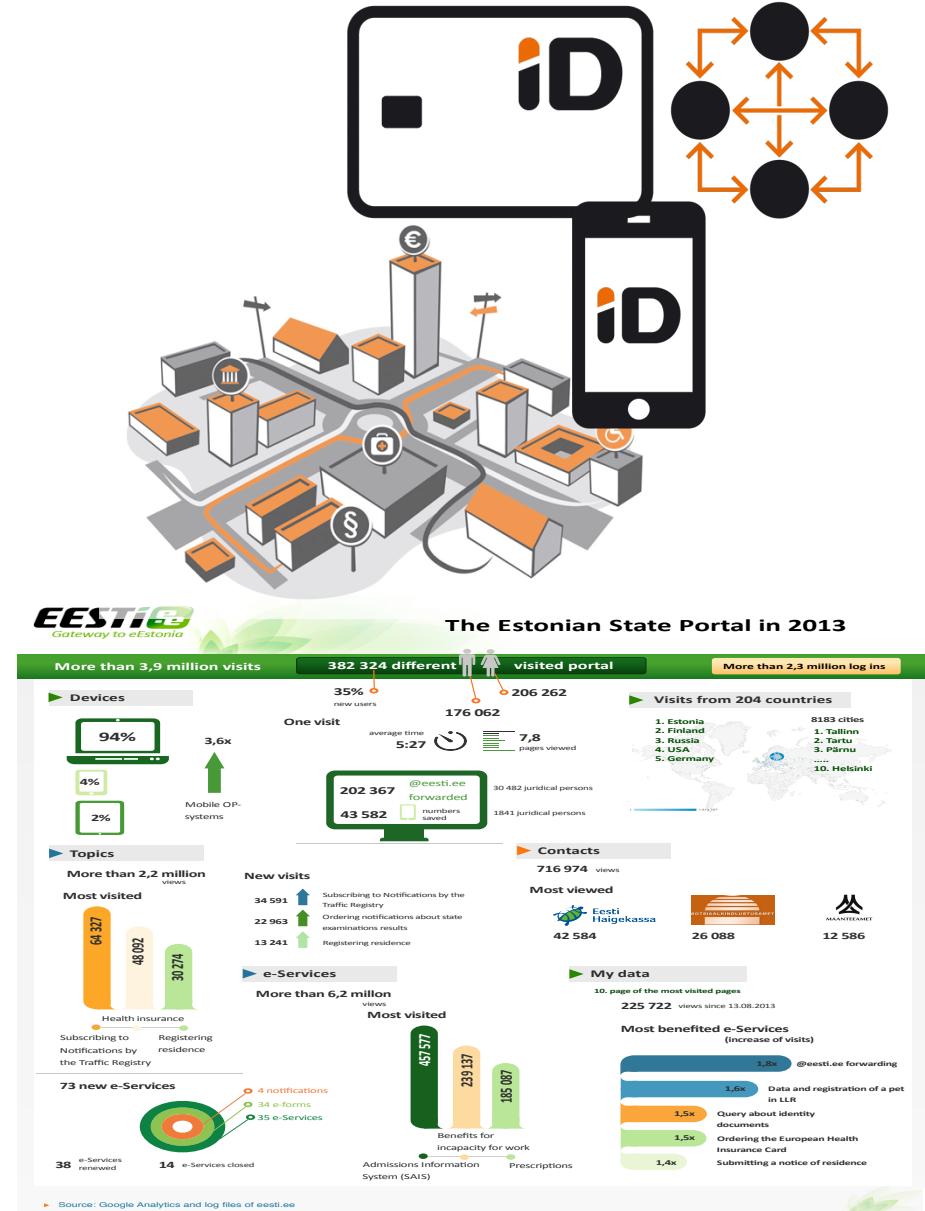
Government Security Committee

National Cyber Security Council

Incident management:

CERT-EE ,GovCERT-EE

National Security Domain and Law Enforcement

Crisis Management

Cyber Defence League
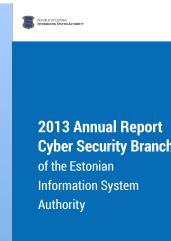
Co-ordination with Cyber Security Policy actors – Ministries and Private sector

The Ministry of Economic Affairs and Communications (lead)

Community building:

CIIP Council

CISO(Gov.) Council

R&D Council

Cyber Security Advisory Board

Trainings

Preparedness and Regulatory supervision:

National level risk and vulnerability analysis

Planning for large scale cyber incident

Stages of alertness

Obligatory reporting

Exercises

Focus: capability to Prevent, Manage & Learn

Estonian Information System Authority manages <u>large scale cyber incidents</u> on State level :

- CERT-EE (https://www.ria.ee/cert-estonia) includes also GovCERT officer

- Incident Response: triage, coordination & resolution

- Obligatory reporting of incidents by

  - *Providers of Vital Services*

  - *Owners of public databases/Government authorities*

  - *Providers of services of electronic communications*

- Management and coordination of State-level emergency situation, including engaging partners like Cyber Defence League (http://www.kaitseliit.ee/en/cyber-unit)

KÜBERKAITSELIIT
ESTONIAN CYBER DEFENCE LEAGUE

Focus: capability to Prevent, Manage & Learn

- National level risk and vulnerability analysis
- Security assessments & testing
- Rules & Regulations (e.g.,baseline)
- Planning for state-level emergency situation
- Support, Review & Supervision

- Community & Competence building
- Know (& share) your Risk Environment
- Know (& share) your best practices
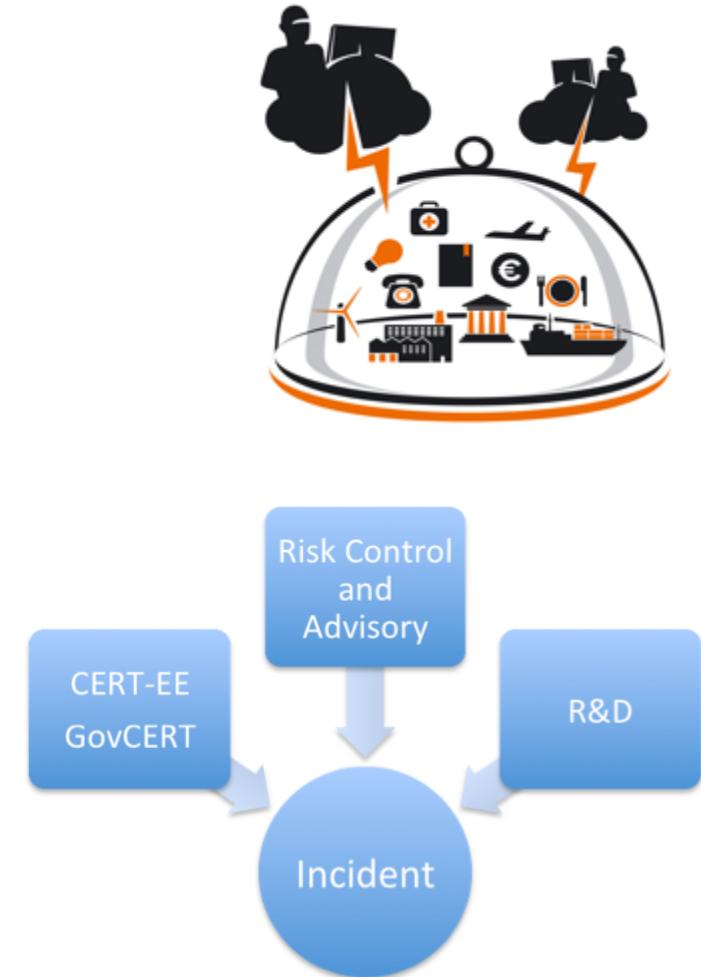
Community Based Approach

CISO's CISO Council	Vital Service Providers CIIP Council
Cyber security advisory board R&D Council	IT managers System administrators

Cyber Security Branch
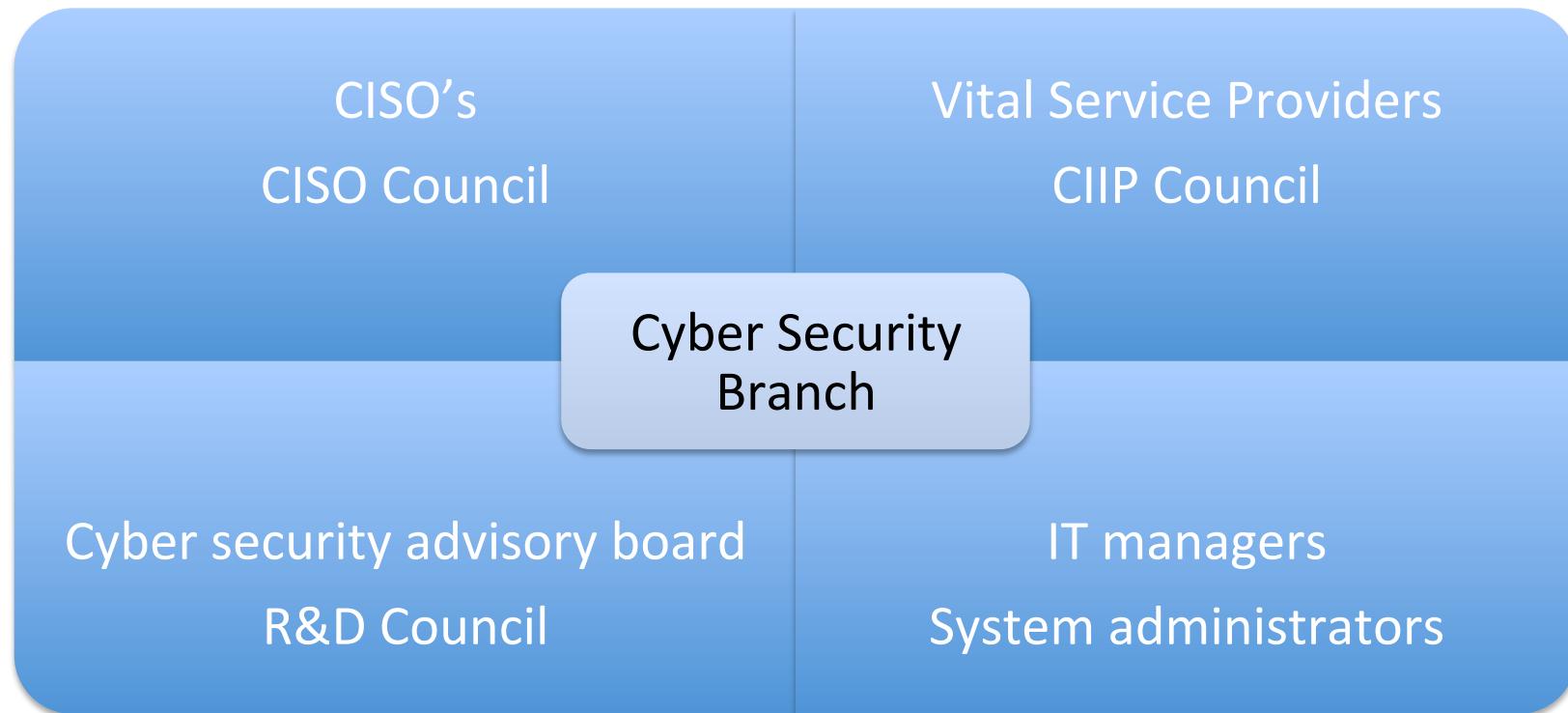
- ➤ **10+ trainings /year**
- ➤ **Appr 20 guidance papers /year**
- ➤ **Regular formal meetings**
- ➤ **Regular / unregular unformal meetings**

Anonymous Ukraine
@freeukraineanon

Ministry of Defence of Estonia tango down!
kaitseministeerium.ee #OpIndependence
continues! pastebin.com/jQ73ETes

← Reply ⇄ Retweet ★ Favorite ••• More

1
FAVORITE

11:05 AM - 1 Nov 13

Reply to @freeukra...

An0nym0us
Ukraine

#OpIndependence

An0nym0us
UA

Check it out on
YouTube
and
Pastebin

CCDCOE
Cooperative Cyber Defence
Centre of Excellence

VS

КИБЕРБЕРКУТ
МЫ НЕ ЗАБУДЕМ МЫ НЕ ПРОСТИМ

Risk Management (lifecycle)

- **Regulatory Supervision**
- **Sec/pen testing**
- **Advisory**
- **Community building**

- **National level risk and vulnerability analysis**
- **Security assessments & testing**
- **Exercises**
- **Reports**
Incidents

Risk review & Measure

Risk Intelligence & Assess

Manage & implement Controls

Risk assessment & Evaluate

- Regulatory Supervision
- Incident management
- Trainings
- .ee monitoring
- Rules & Regulations (e.g. baseline)
- Community building

- **Analysis & segmentation by RIA**
- **Exercises**
- **Incidents**

Layers of Defense

Country → Critical Infrastructure, Essential & Vital services ?

Organisation → Process

Community → Culture

Person → Hygiene

Cyber defense is a total defense

Future

- Growing complexity $\rightarrow$ challenges
- Growing dependency (& interdependencies)
- Isolation is expensive stagnation
- People are important
- The best collective brain wins

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Thank You!

Sven Kivvistik

sven.kivvistik@ria.ee

www.ria.ee

https://www.ria.ee/about-estonian-information-system-authority/