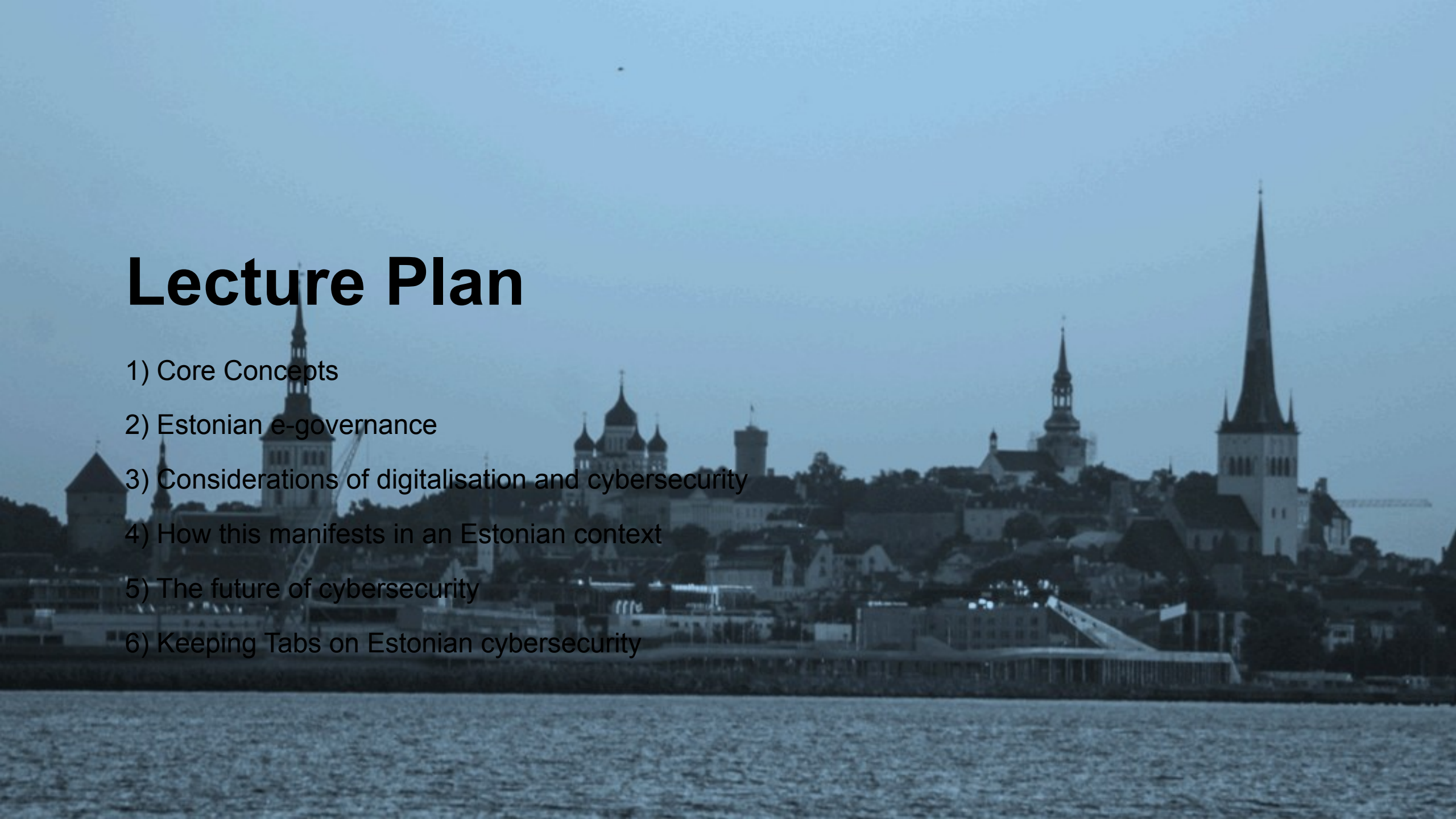
e-Governance & Cybersecurity in Estonia

Logan Carmichael
University of Tartu (Estonia)
6th November 2024



Lecture Plan

1) Core Concepts

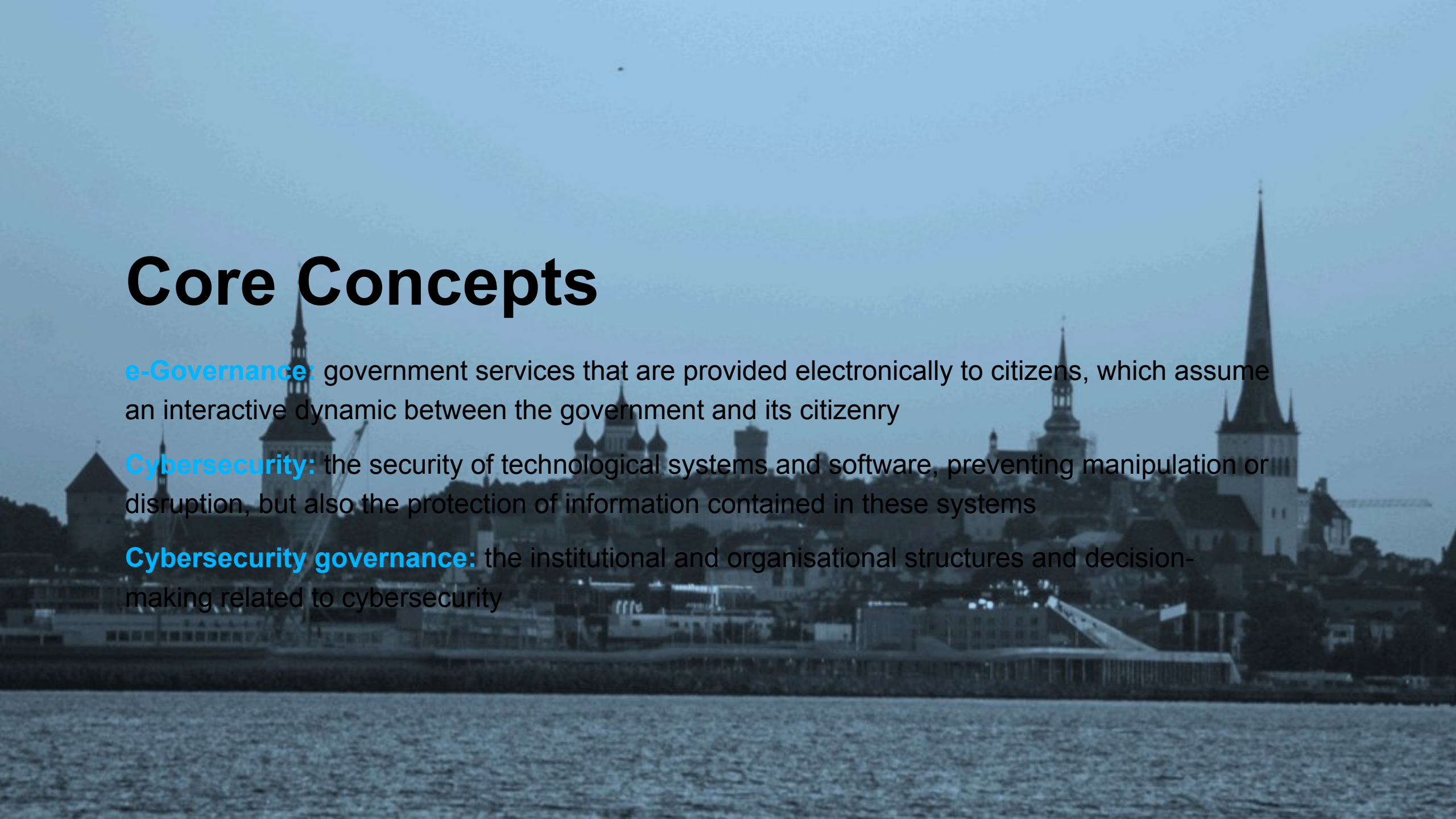
2) Estonian e-governance

3) Considerations of digitalisation and cybersecurity

4) How this manifests in an Estonian context

5) The future of cybersecurity

6) Keeping Tabs on Estonian cybersecurity



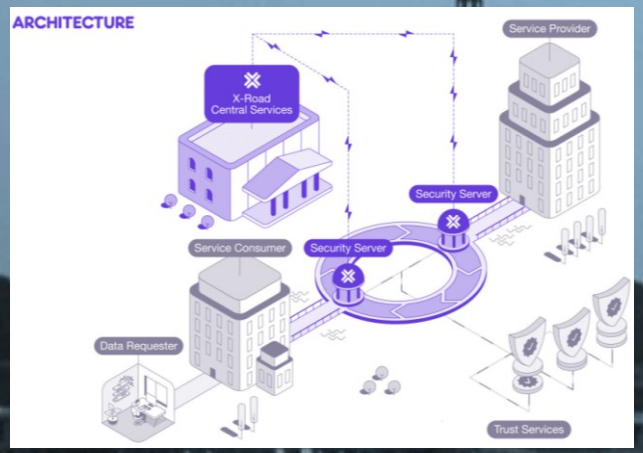
Core Concepts

e-Governance: government services that are provided electronically to citizens, which assume an interactive dynamic between the government and its citizenry

Cybersecurity: the security of technological systems and software, preventing manipulation or disruption, but also the protection of information contained in these systems

Cybersecurity governance: the institutional and organisational structures and decision-making related to cybersecurity

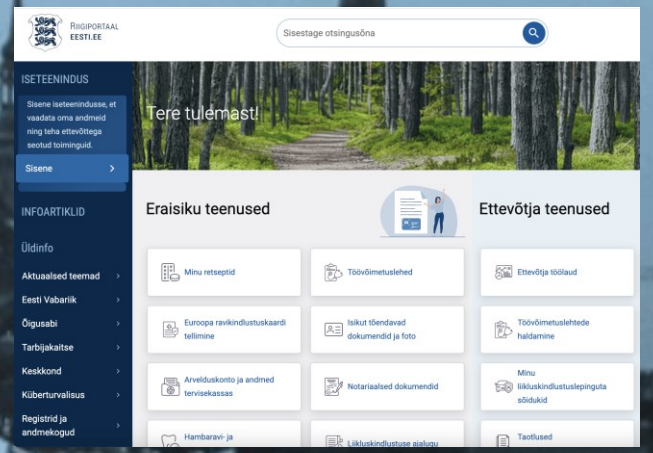
What are the core elements of Estonian e-governance?



X-Road

Electronic Identification (eID)

Internet Voting



eesti.ee portal

Digitalisation  Cybersecurity

How are digitalisation and cybersecurity interconnected? What must be considered when securing e-governance provisions?

Technology

- Appropriate technology for the current threat landscape; constant investment and improvement
- Sufficient technical expertise

People/Users

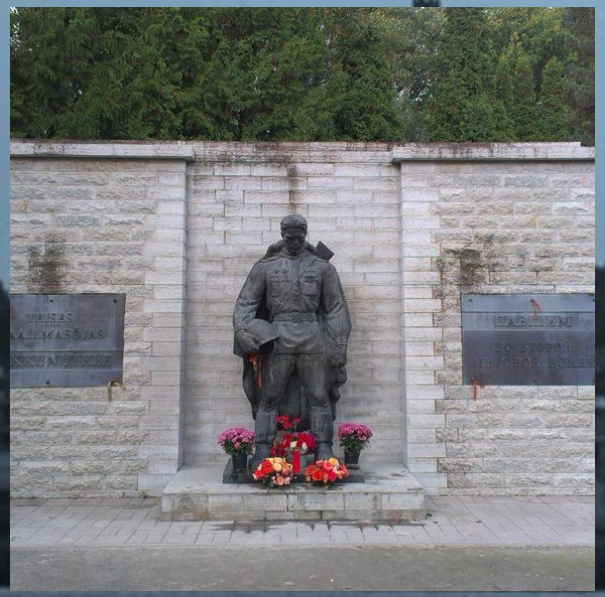
- An overwhelming # of cyberattacks have preyed on the average person's lack of tech and cyber hygiene awareness
- How can you train the general public? Social media? Radio? TV? News print?

Decision-Makers

- Ultimately responsible for technology and users
- Large number of stakeholders involved, and typical public-private partnerships
- Shift from elected officials to tech implementers as decision-makers

Case Study: 2007 Cyberattacks

Removal of monument → Political violence in Tallinn → Cyberattacks on key websites



BBC NEWS

Watch One-Minute World News

News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment
Technology

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

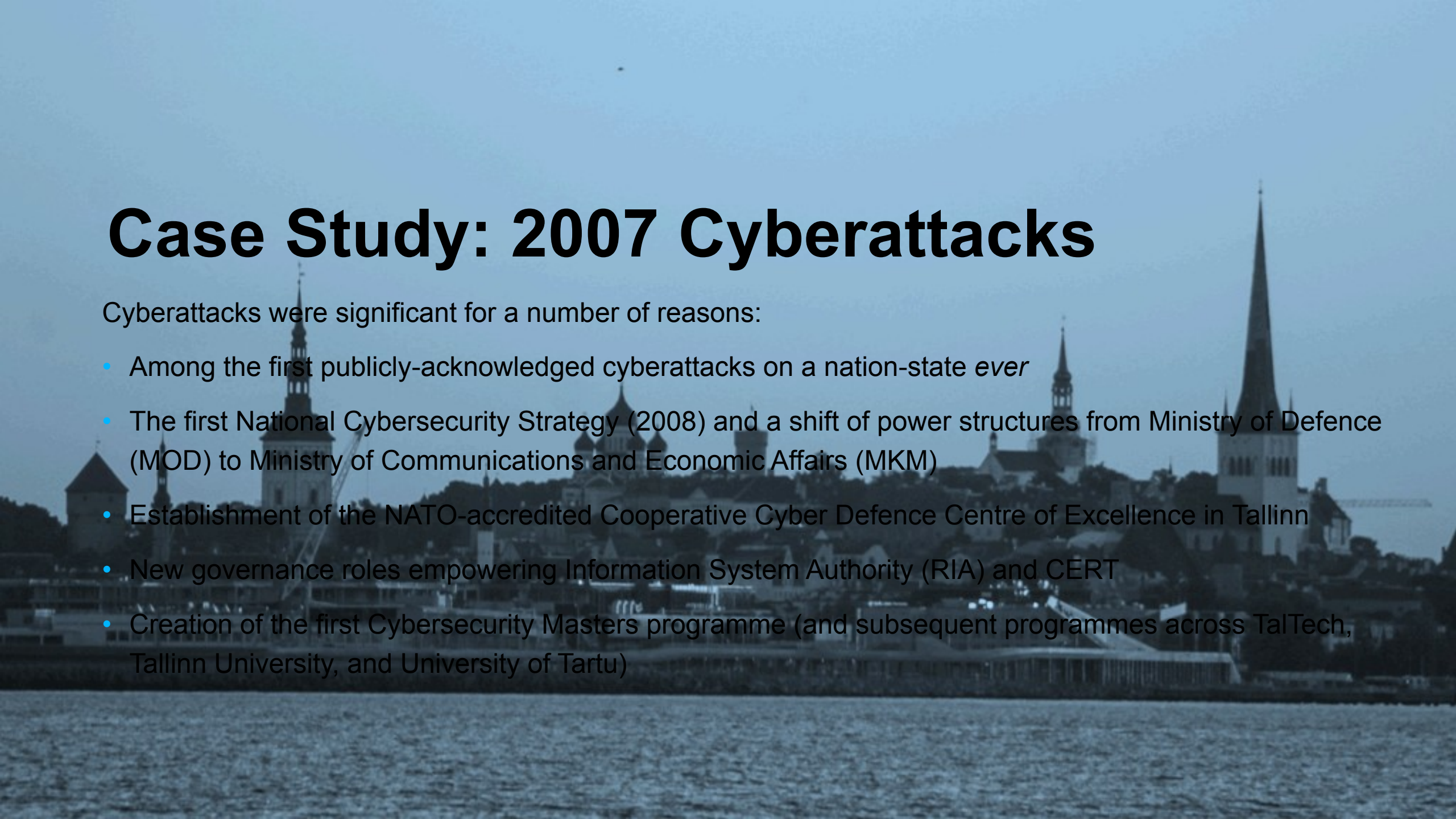
E-mail this to a friend Printable version

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

Estonia says many state websites have been affected



Case Study: 2007 Cyberattacks

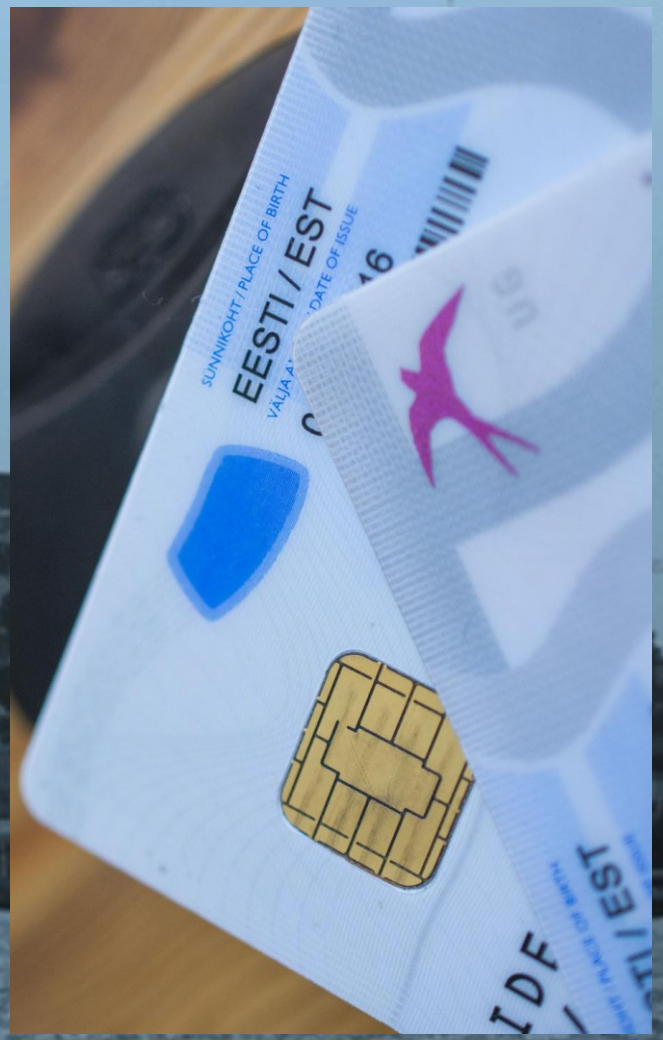
Cyberattacks were significant for a number of reasons:

- Among the first publicly-acknowledged cyberattacks on a nation-state *ever*
- The first National Cybersecurity Strategy (2008) and a shift of power structures from Ministry of Defence (MOD) to Ministry of Communications and Economic Affairs (MKM)
- Establishment of the NATO-accredited Cooperative Cyber Defence Centre of Excellence in Tallinn
- New governance roles empowering Information System Authority (RIA) and CERT
- Creation of the first Cybersecurity Masters programme (and subsequent programmes across TalTech, Tallinn University, and University of Tartu)

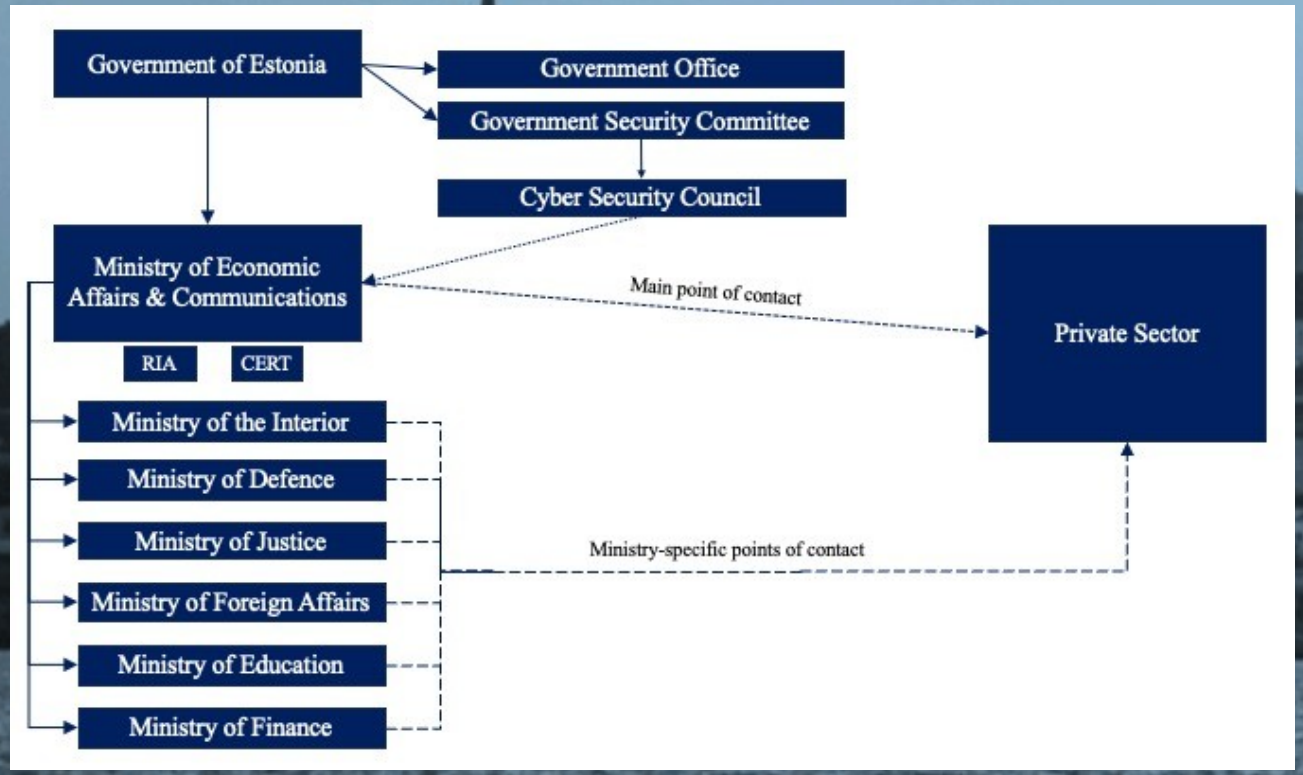
Case Study: 2017 eID Crisis

Key generation vulnerability→ Government announcment of crisis→ Patch found and crisis averted

- Czech researchers found a ‘return of the coppersmith’ vulnerability in eID cards of 800,000 Estonians (as well as in Austria, Spain, and elsewhere)
- Clear and transparent government communications while a patch was sought
- Upcoming local elections, as well as fears of fraudulent activity; dark web monitored for exploits
- Patch found and deployed by RIA, ’crisis’ did not eventuate



Configuring Cybersecurity Governance



- There is not a “Ministry of Cybersecurity” and, thus, cybersecurity matters must sit between several government bodies
  - Cyber Security Council = high level decision-making body, which has gained significant cybersecurity know-how over time
  - National Cyber Director sits atop MKM
  - RIA and CERT also hosted within MKM; most sophisticated technical capacity for cybersecurity
- Shifts in structure from July 2024
  - Ministry of Justice in elevated role

The Future of Digitalisation & Cybersecurity

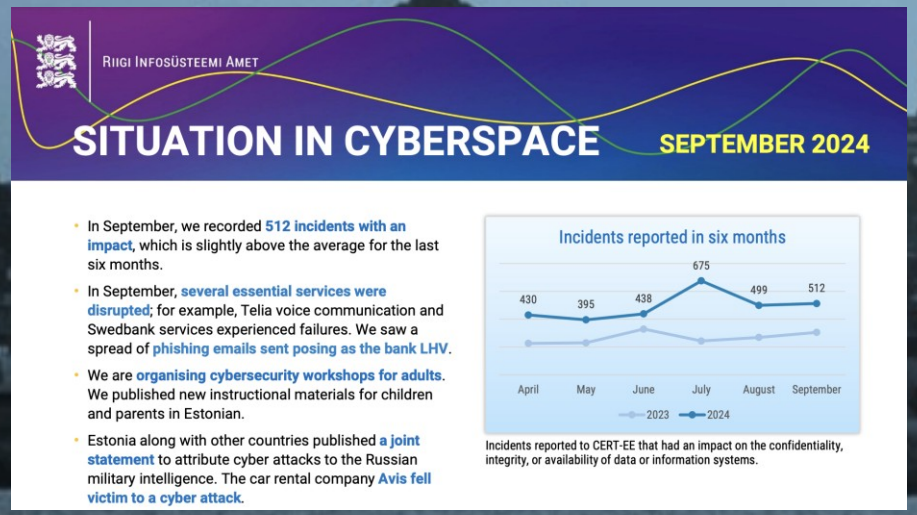
Cybersecurity is ever-evolving, and never guaranteed:

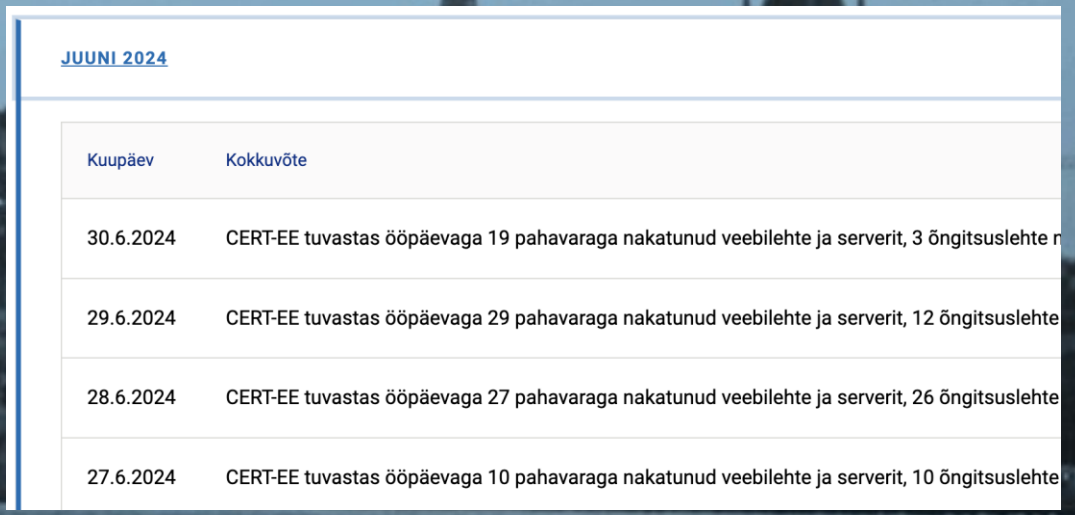
- As countries across the world continue to digitalise, their ‘surface area’ for cyberattacks also increases
- In the past half-decade, cyberattacks have increased in their frequency and sophistication
  - While DDoS was a major concern in 2007, technology has improved, but malware attacks, including ransomware, are on the rise
- Estonia will face new challenges by providing its state services portal via a mobile app, as well as its future introduction of mobile internet voting

Keeping Tabs on Estonian Cybersecurity

RIA does rigorous daily, monthly, and annual reporting on the state of cybersecurity in Estonia, alongside global trends and threat landscapes

https://www.ria.ee/en/cyber-security/cyberspace-analysis-and-prevention/situation-cyberspace#





Thank you for your attention! Questions?

Let’s keep in touch!

logan.emily.carmichael@ut.ee