

# e-Governance & Cybersecurity

Logan Carmichael

University of Tartu (Estonia)

6th November 2024



# Lecture Plan

Core Concepts

What does e-governance look like?

What are the cybersecurity considerations around e-governance?

What does this look like in action?

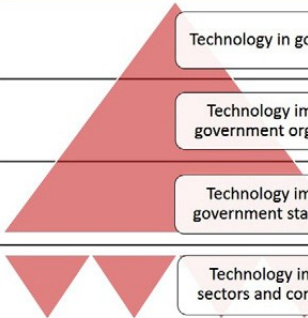
The future of cybersecurity and e-governance

# Core Concepts

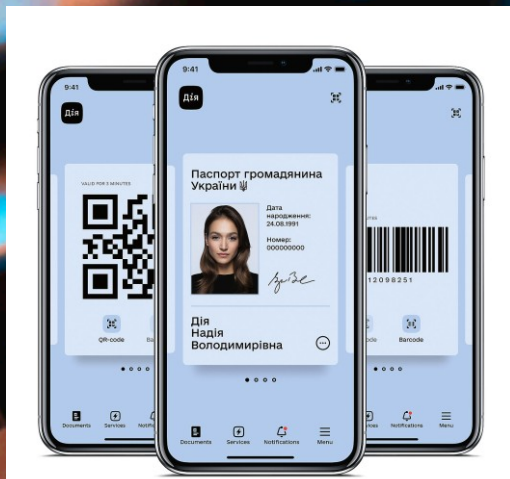
**e-Governance:** government services that are provided electronically to citizens, which assume an interactive dynamic between the government and its citizenry

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

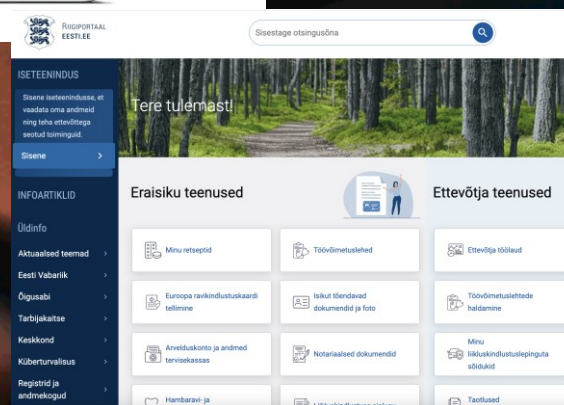
**Cybersecurity governance:** the institutional and organisational structures and decision-making related to cybersecurity

STAGE	APPLICATION CONTEXT	CHARACTERIZATION		
		Internal government transformation	Transformation affects external relationships	Transformation is context-specific
Digitization	 Technology in government	no	no	no
Transformation	Technology impacting government organization	yes	no	no
Engagement	Technology impacting government stakeholders	yes	yes	no
Contextualization	Technology impacting sectors and communities	yes	yes	yes

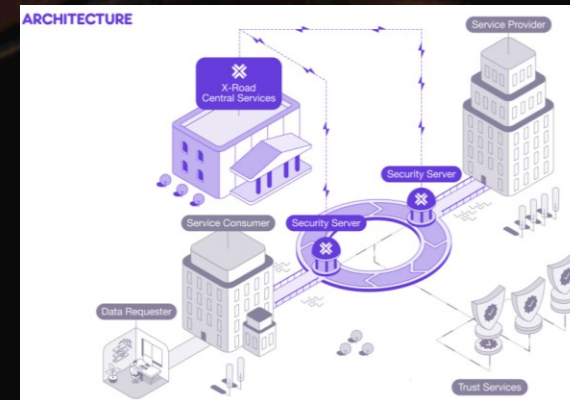
# What does e-governance look like?



Internet voting



Service platforms/portals



Data Exchange Platforms

Electronic Identification (eID)

# e-Governance and Cybersecurity

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

**Systems/  
Technology**



**People/Users**



**Decision-Makers**

# Systems/Technology

- Appropriate technology for the cybersecurity threat landscape
  - Routine security updates, all the way up to large-scale softwares and infrastructures
- Constant investment and improvement into technologies (this is linked with decision-makers, who typically must sign off on funding)
- Sufficient technical expertise to maintain systems and deal with incidents

**e-Governance case study:** internet voting – cryptographic setup, vote recast, authentication methods, desktop vs. mobile voting

# People/Users

- The average user of e-governance provisions does not have training in cybersecurity or related fields, but a great deal of onus falls on them
- Cyberattacks often prey on this lack of tech and cyber hygiene awareness
- How can you train your citizenry? How do you deliver messaging? These are also questions for decision-makers
- **e-Governance case study:** governments have attempted to run information campaigns on various platforms, but there is not yet a surefire way to broach this

# Decision-Makers

- Ultimately responsible for technology and users
- Large number of stakeholders involved, across government ministries/agencies, as well as private sector via public-private partnerships
- Shift to an increased role of software designers as decision-makers

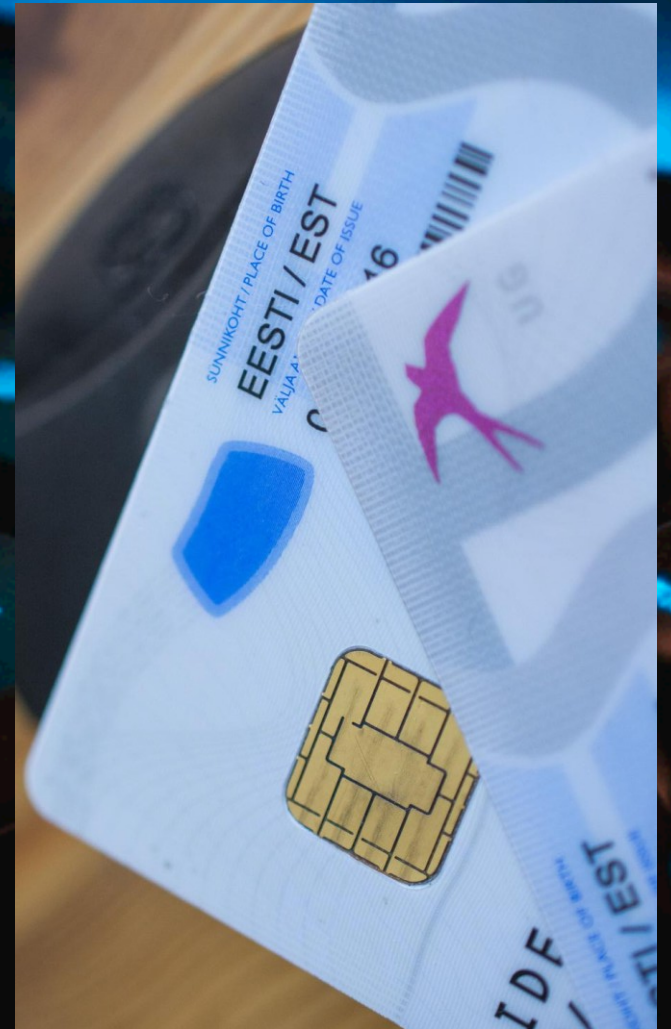
**e-Governance case study:** AI uses in e-governance; when implemented, typically politicians or bureaucrats do not have the expertise to configure artificial intelligence implementations, therefore the software designers play an elevated role; also decision to delay mobile internet voting



# e-Governance & Cybersecurity in Crisis: Estonia's eID Crisis

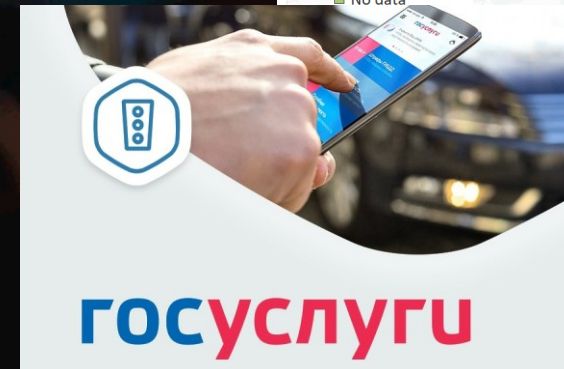
Key generation vulnerability → Government announcement of crisis →  
Patch found and crisis averted

- 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



# The Future of e-Governance and Cybersecurity: Non-Democracies

- e-Governance provisions are increasingly being used in non-democratic settings
  - Internet voting in Russia
  - Gosuslugi portal in Russia
  - Biometrically enabled eID in China
- Russia and China see themselves as diffusers of technological innovations in their neighbourhood



# The Future of e-Governance and Cybersecurity

Cybersecurity is ever-evolving, and never guaranteed:

- As countries across the world continue to digitalise, their 'surface area' for cyberattacks also increases
  - Rollout of entirely new digital governance systems (ie. Oman), or new versions of various services (ie. Estonia and mobile eesti.ee app, later i-voting)
- 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

# Thank you for your attention!

## Questions?

Let's keep in touch!

[logan.emily.carmichael@ut.ee](mailto:logan.emily.carmichael@ut.ee)

