Emerging Cyber Surveillance Threats
SIG-ISM – WISE workshop
2021-05-25
Urpo Kaila, Head of Security (CSC)
Information Security Risk Officer (EOSC-Future)
Security Officer (EUDAT)
We have a long history to cope with threats related to

• System compromise
• Compromised accounts
• Software vulnerabilities
• Weak configurations
• Inadequate credentials
Recap of terms

- Vulnerability – A weakness that can be exploited
- Threat - A circumstance or event with potentially adverse business impact
- Exposure – A combination of likelihood and impact for a risk
- Risk – Effect of uncertainty of objectives, business impact
- Control – Technical and/or administrative means to managing risks
- Mitigation – A strategy to reduce risks to an acceptable level
Political risks

• Political risks can significantly affect the viability of our infrastructures

• Changes in national and international conditions can have major business impacts:
  
  o Funding
  o Regulation
  o Conditions for procurement
  o Compliance requirements
    o Information Security
    o Data Protection
    o Critical infrastructure
  o Economic sanctions and international trade disputes
  o Export regulation for vital technology
Risks related to cyber surveillance and information warfare (1/2)

• Advance persistence threats
• Surveillance laws, access to infrastructure
• Blacklisting of companies and citizens from certain countries
• Politicization of infrastructure projects
• Challenging requirements on security compliance
Risks related to cyber surveillance and information warfare (2/2)

• Restrictions on data transfers (GDPR etc)
• Requirements for security clearances
• Rising international tensions
• An emerging market to exploit vulnerabilities and data leaks
• Active surveillance and intrusion attempts by government cyber agencies
How to mitigate risks on cyber surveillance?

• Security housekeeping, keep your services secure (basic level at least)
• Proactive security (IDS/IDP, monitoring)
• Raising your security level (MFA, Secure terminal devices, securing your own infrastructure)
• Limit open an public access to services?
• Re-evaluate trust in federated identity providers?
• Avoiding controversial providers?
• Divert decision making to authorities?
• Take the risk
What do YOU think?

Go to www.menti.com and use the code 56 59 74 7