What is IT security?

- Clean desk policies
- Attached files
- Information security management system (ISMS)
- Ransomware
- Phishing
- DoS-attacks
- Industrial espionage
- Malware
- Virus
- Identity thefts
Digitalisation is about communicating and sharing information through Internet

...with the help of Information and Communications Technology (ICT)

Software  USB  Printers  Smart devices
Why is IT security regulation so important now?

• Number of people online and communicating through Internet increase all the time

• The number of security incidents and attacks increase and entail more and more serious consequences

• There is a false security and reliance in the system
Incidents and attacks...
https://threatmap.fortiguard.com/

545,000
NETWORK INTRUSION
ATTEMPTS
resisted per minute
Why does the National Board of Trade analyse the subject?

Cybersecurity regulation has a major impact on the trade of ICT and risk to generate more barriers to trade!
Cyber regulation as a policy challenge

NATIONAL SECURITY
REGULATORY OBJECTIVE:
TO PROTECT THE STATE AND ITS CITIZENS AGAINST ALL KINDS OF NATIONAL CRINES

TRADE POLICY
REGULATORY OBJECTIVE:
TO PROMOTE FREE TRADE AND MARKET ACCESS WHILE RECOGNISING THE RIGHT TO REGULATE TO PROTECT SAFETY, HEALTH, ENVIRONMENT AND NATIONAL SECURITY
How can IT security be addressed through regulation?

- Requirements on IT-products
  - Product requirements
  - Requirements on conformity assessment (certification/evaluation)
To what extent is IT security in ICT regulated?

- National Security
- Goods within critical infrastructure
- Commercial IT products
How can IT security be managed through regulation?

• Requirements on IT-products
  - Product requirements
  - Requirements on conformity assessment (certification /evaluation)

• Requirements on IT infrastructure
The very same IT products are manufactured, sold, installed and used all over the world

= Internationally harmonised regulations and standards for IT security?
Regulatory fragmentation with trade effects

- Strategies for IT security regulation is actualised in national and regional strategies and national specific requirements
- Regulatory fragmentation may risk more trade barriers without the possibility to form an objective opinion if the specific national or regional requirements are effective and relevant
Regulatory fragmentation?

- Product requirements that are based on national technical regulations
- Specific national certification requirements

Technical Barriers to Trade (TBTs)
Why do various countries have different views on IT security regulation?

- Perception of national assets or critical information
- Capabilities (technical knowledge and infrastructure) to protect assets and critical information

These two parameters are extremely difficult to harmonize internationally!
International regulatory cooperation and policy initiative within the EU

+ International standard for cyber certification with mutual recognition of certificates

- Standard is generic and creates a need for additional national requirements

+ The focus in the EU Internal Market regulation so far on infrastructure requirements

- New EU regulatory tools will embrace product specific requirements but not necessarily in line with the EU system for technical harmonisation or international systems
Existing regulatory strategies- PROs and CONs

- Status quo

- Requirements on cyber certification of ITC

- Requirements on the infrastructure where ICT is used
Cyber regulation as a policy challenge
Conclusions

• Regulatory initiatives that concern IT security of ITC are extremely important!

• Regulatory initiatives on IT security for ICT embrace several policy areas which require a holistic perspective!

• It is necessary to analyse regulatory initiatives from a trade perspective!
Recommendations

CYBER STRATEGY

- Improved knowledge
- Strengthened dialogue

TRADE

NATIONAL SECURITY

BUSINESS
ASSETS, INNOVATIONS, DEPENDENCIES, VULNERABILITIES

SOCIETY
CRITICAL INFRASTRUCTURE, INFORMATION ASSETS, VULNERABILITIES

INTERNATIONAL
Regulatory Initiatives
Trends and issues to follow

Privatisation of critical infrastructure services

- The state has less and less control of service providers IT solutions
- The cyber landscape and priorities of individual countries different
- Each country is forced to evaluate policy options e.g. in the EU/INT carefully
- To manage or even coordinate cyber resilience through regulation within EU e.g. is likely to be more demanding than coordination in another policy domain!
Trends and issues to follow

In the field of cybersecurity of ICT: regulatory fragmentation rather than regulatory harmonisation

- Need to evaluate trade dependencies in relation to regulations
- Small countries might suffer from regional/ international regulatory solutions not taking their trade partners conditions into account
- It can be expected that countries become “less loyal” to policy principles as they see cybersecurity partly falling in the scope of national security!
- Some part of incident reports and harmful cyber activity might fall off the radar!
Trends and issues to follow

Privatization of regulation

- Public-private partnerships will be essential – as ICT regulation (standardization) is more and more driven by business, and in sector specific communities

- An increased insight in sectors and technologies are also vital for evaluation of new draft regulations as well as for the enforcement of legislation (which is a challenge in cyber as such)

- There is a need to more closely follow standardisation initiatives in the field of cybersecurity to for a holistic view on where technology is moving!
How about regulatory tools to be used?

- Nothing connected to Internet is safe!

- Cyber certification may raise cybersecurity but only if countries can mutually agree on certification schemes that prove to cover prioritized (often inter linked) vulnerabilities.

- It is reasonable to expect that countries have strong national interests - which might result in "standards wars" - why the policy makers should consider relying on regulatory schemes with open, transparent standards setting!
Cybersecurity requirements - how?

The success in addressing cybersecurity in ICT are dependent on

- Improving the knowledge and skills of cybersecurity in general by the creation of strong security culture overall – tools such as regulatory frameworks such as NIS are good for raising cyber resilience for vital society functions
- Shifting the focus of security measures as far as possible to the initial stage of product life cycle:

  although complex to address by technical regulation..
Thank you for your attention!

Heidi.Lund@kommers.se