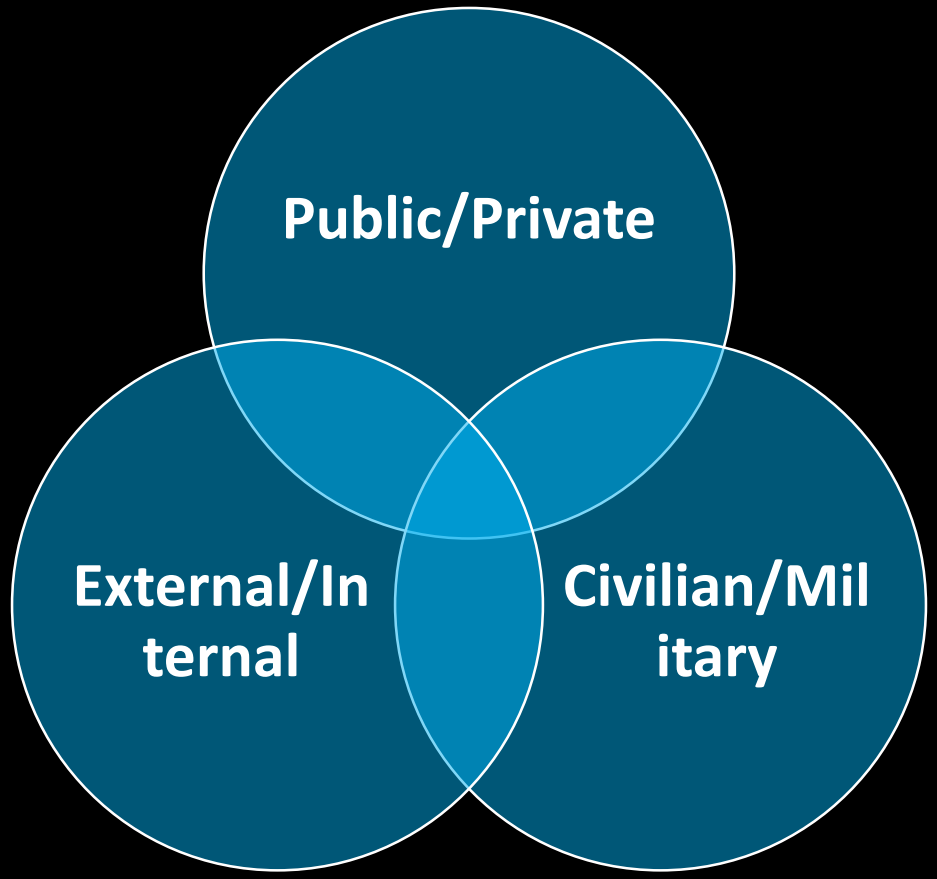
Paradigm Shift in European Cybersecurity

Agnes Kasper, PhD

TalTech

III Kharkiv Legal Forum 26. September 2019

Entanglement of domains in cybersecurity



WannaCry and Petya/NotPetya attacks 2017

- Leveraged NSA-stockpiled **vulnerability**, Eternal Blue expoit (stolen in 2017) Patch available since 14.March 2017
- Wannacry & Petya → **ransomware**
- NotPetya → designed to **destroy**, not to extort
- Petya/NotPetya → Ukrainian tax accounting sw MeDoc used as trojan
- Encrypted data worldwide **indiscriminately** – crippled systems incl. Chernobyl Nuclear Power Plant, UkrTelecom, State Savings Bank of Ukraine, Kyiv International Airport, Deutsche Bahn, Telefonica, Vodafone, UK hospitals, Maersk, FedEx, Boeing, etc.
- Wannacry →US+UK **attributed** publicly to North Korea
- Petya/NotPetya → Ukraine, US, UK attributed to Russia

White House reaction

Statement from the Press Secretary, February 15, 2018

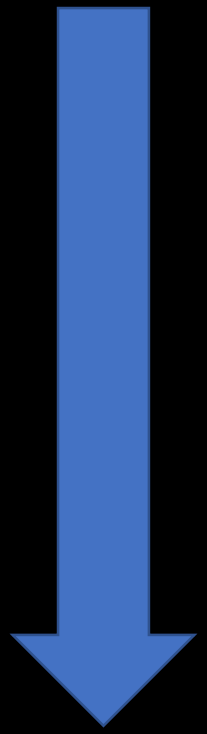
"In June 2017, the Russian military launched the most destructive and costly cyber-attack in history.

The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences."

https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/

Unfolding complexity of cybersecurity policy

Economic and privacy issues



1994 Bangemann report

1995 Personal Data Protection Directive

2001 Council of Europe Cybercrime Convention (EU follows developments)

…

2013 EU Cybersecurity Strategy → focus dominantly on threats to single market

2017 EU Cybersecurity Strategy → focus on economic, political and military threats

National security and strategic autonomy

BUT! Subsidiarity

*"While **Member States remain responsible** for national security, the scale and cross-border nature of the threat make a powerful case for **EU action providing incentives and support** for Member States to develop and maintain more and better national cybersecurity capabilities, while at the same time building EU-level capacity"*

Joint Communication Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 13.09.2017 (2017 EU Cybersecurity Strategy)

Issues

I. Subject-matter clarity (5w&h)

- makes a difference for regulatory framework, i.e. what is the scope of EU cybersecurity policy and what is EU cybersecurity law?

II. EU competences in security matters

- makes a difference for EU integration, governance architecture and external cooperation

2013 EU Cybersecurity Strategy

Only working definition in footnote 4:

“safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or may harm its independent networks and information infrastructure”.

2015 ENISA definition?

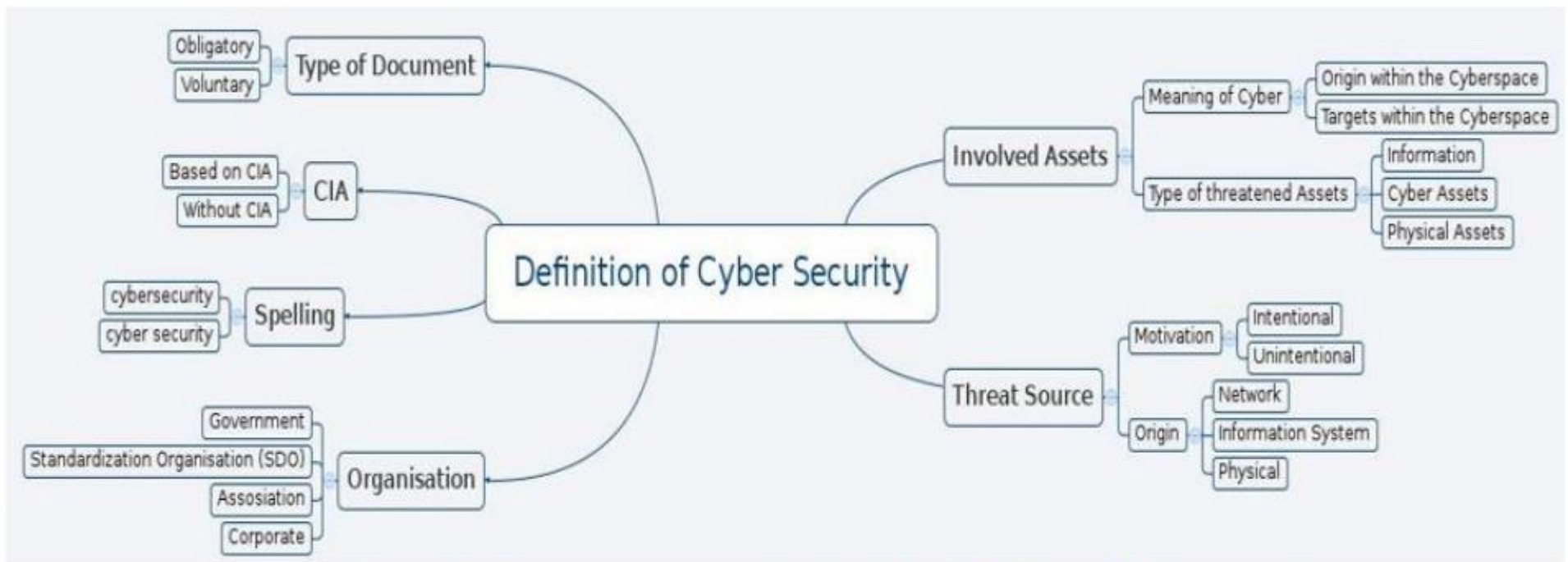


Figure 2: Components constituting the definition of Cybersecurity

"The problem is that Cybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers."

Cybersecurity Act (Regulation (EU) 2019/881)

Article 2 defines cybersecurity for the purposes of the act as “all activities necessary to protect network and information systems, their users, and affected persons from cyber threats”

New scope? ***Protection of persons***, not only cyberspace in itself.

Focus shifts to ***interactions*** between persons and computer systems.

Protection from what harms?

Harms identified (based on 2017 EU Cybersecurity Strategy, etc.)

Systems

Compromise of

- Confidentiality,
- Integrity
- Availability
- Authenticity
- Non-repudiation

Persons (implies individual/society)

- Negative economic impact of misuses and degradation in the functioning of computer systems;
- Decrease in consumer trust;
- Economic destabilization;
- Decreased political autonomy;
- Harms arising form disrespect for territorial integrity of states;
- Physical harms;
- Decrease ability of states to provide order in the society by enforcing their laws.
- Others?

Challenges

- **Overlaps** among several sectoral and generic policy domains, i.e. telecom, personal data protection, consumer protection, payment services, critical information infrastructure protection, cooperation in criminal matters, Common Foreign and Security Policy/Common Security and Defence Policy
- Balance between **privacy and security** measures (see CJEU *Tele2 Sverige*, C-203/15)
- Strategic **autonomy** goal vs dependence of the EU on external hw/sw providers
- Resilience building vs **militarization** of cyberspace
- **Motivation** of actors (profit oriented private sector vs public sector)
- **Expertise** and ownership
- Access to policy-making and channels for participation in **governance**

EU CYBERSECURITY POLICY

Resilience

- ENISA
- Single Cybersec. market
- NIS Directive
- Rapid emergency response
- Competence network and centre
- Cyber hygiene and awareness
- Cyber skills
- Duty of care principle
- Security by design
- Etc.

Deterrence

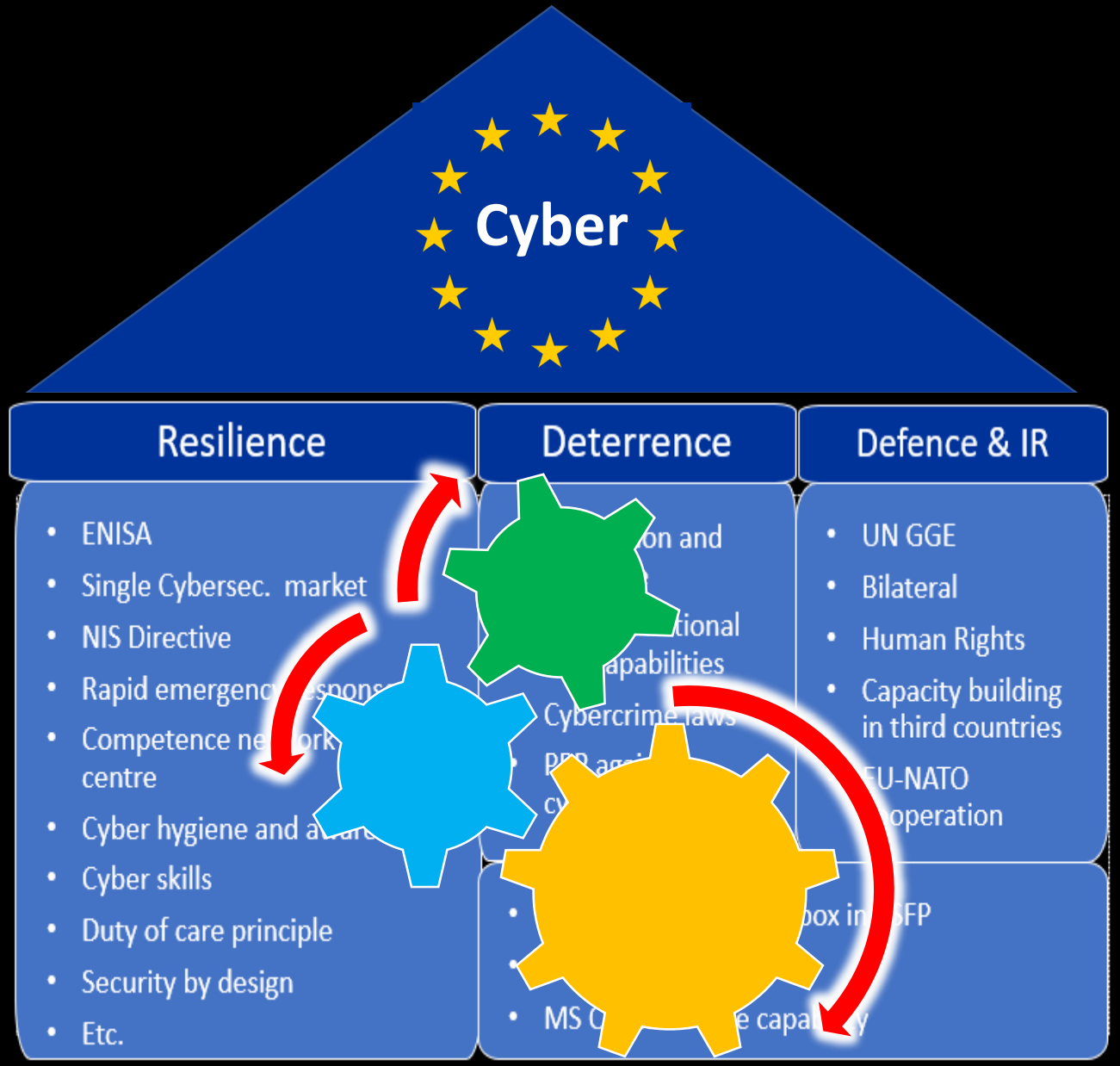
- Attribution and evidence
- EC3 and national LEA capabilities
- Cybercrime laws
- PPP against cybercrime

Defence & IR

- UN GGE
- Bilateral
- Human Rights
- Capacity building in third countries
- EU-NATO cooperation

- Cyber Diplomacy Toolbox in CSFP
- EU Crisis Response
- MS Cyberdefence capability

Towards a ‘Cyber Maastricht’?



Conclusions

- Clarify the 5w&h of cybersecurity → both at national + EU levels
- Integrate policy according to dependencies and functional linkages

References

- Kasper, A, Antonov, A (2019) T'owards Conceptualizing EU Cybersecurity Law' - ZEI Discussion Paper C 253 / 2019. Bonn, Germany: Center for European Integration Studies, Universität Bonn. https://www.zei.uni-bonn.de/publications/zei-discussion-paper-1

Forthcoming:

- Kasper, A (2020) 'EU Cybersecurity Governance – Stakeholders and Normative Intentions towards Integration'. In Moncada, S. (ed.) Future of Europe
- Kasper, A, Vernygora, V (2020) 'Towards a 'Cyber Maastricht': two steps forward, one step back'. In Moncada, S. (ed.) Future of Europe.
- Kasper, A., Mölder, H (2020) 'The EU's Common Security and Defense Policy in facing new security challenges and its impact on cyber defence'. In Troitiño, D, Kerikmäe, T, Perez, G, Martin, R (eds.) The EU in the 21st Century – Challenges and Opportunities for the European Integration Process. Springer.

Thank you!
Questions?