University of BRISTOL

PolicyBristol

Regulating digitisation of critical infrastructures: recommendations to harmonise safety and security of Operational Technologies

Dr Ola Michalec, Dr Sveta Milyaeva, Prof Awais Rashid (University of Bristol)

About the research

As digital innovations proliferate across critical infrastructure sectors, we begin to regulate them to ensure the reliable and safe delivery of essential services like water, energy, or transport. The Network and Information Systems Security (NIS) Directive, implemented across the EU and the UK, is a prime example of such efforts. It is a novel regulatory response to the increased interconnection of industrial computers to the internet.

Our research, based on interviews with 30 cyber security practitioners conducted in 2020 and 2021, uses the case study of the UK's NIS Regulations to identify good practices and remaining challenges. We found that the implementation of NIS is the first step to integrate safety and security through novel risk management practices observed in our fieldwork, such as broadening of threat and incident reporting scope to include security incidents and safety accidents. However, we also show that security risk management practices cannot be directly transplanted from the safety realm. This is because cyber security is grounded in anticipation of the future uncertain adversarial behaviours, while safety risk management relies on a long history of data on equipment failure rates. As such, we call for exercising care while transplanting concepts from 'safety culture' into the realm of cyber security.

Recommendations for Competent Authorities:

- Encourage voluntary sector-wide initiatives to benchmark responses to the NIS Regulations;
- Provide reassurance and remove stigma from reporting incidents and vulnerabilities;
- Highlight the overlaps between the NIS Regulations and commonly accepted sector-specific safety guidelines and standards;
- Be cognizant of the cultural differences between safety and security which limit the potential for harmonisation, i.e. prescriptive thinking of safety engineers or secrecy of security practitioners;
- Clarify communications about the aims of Cyber Assessment Framework, i.e., specify whether the document serves the purpose of compliance or independent risk assessment.

Image by Tim Hill from Pixabay

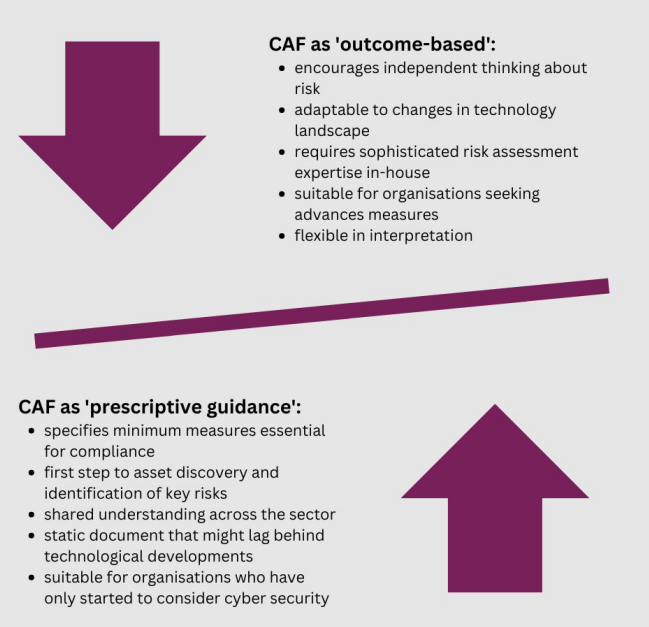
University of BRISTOL

PolicyBristol

Key findings

The NIS Regulations introduced the document called Cyber Assessment Framework (CAF). It is designed as a guidance outlining desired outcomes of good cyber security practices that facilitate independent risk management among the Operators of Essential Services.

However, our research found a paradox regarding the use of CAF. Despite being designed to guide independent risk assessment and discourage 'box ticking', in some cases, CAF has been used as a prescriptive document, outlining exactly what needs to be achieved for compliance. This was justified with poor understanding of industrial assets and associated security risks across the Operators. We argue that outcome-based regulations are more likely to be successful once the stakeholders identify and apply a set of baseline security improvements. Such improvements ought to be benchmarked across the sector, linked to the traditional requirement of safety, and culturally accepted by Operational Technology engineers.



"Advancing cybersecurity of critical infrastructures: outcomes-based Vs prescriptive approach

Further information

Michalec, Ola, Sveta Milyaeva, and Awais Rashid, (2022). "When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures?" Big Data & Society, 9(1), https://doi.org/10.1177/20539517221108369

Michalec, Ola, Sveta Milyaeva, and Awais Rashid. (2021) "Reconfiguring Governance: How Cyber Security Regulations Are Reconfiguring Water Governance." Regulation & Governance, June, rego.12423. https://doi.org/10.1111/REGO.12423.

Michalec, Ola, Dirk van der Linden, Sveta Milyaeva and Awais Rashid (2020) "Industry Responses to the European Directive on Security of Network and Information Systems (NIS): Understanding policy implementation practices across critical infrastructures"; the Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020). https://www.usenix.org/system/files/soups2020-michalec.pdf

Policy Briefing 110: "Regulating digitisation of critical infrastructures: we need diverse experts to translate cyber security risks into the sector-specific contexts" (2021) Ola Michalec, Sveta Milyaeva, Awais Rashid, Policy Bristol http://www.bristol.ac.uk/policybristol/policy-briefings/regulating-digitisation-infrastructure/

Policy Briefing 91: "Regulating digitisation of critical infrastructure: cyber security decisions must be based on robust evidence" (2020) Ola Michalec; Dirk van der Linden; Sveta Milyaeva; Awais Rashid. Policy Bristol http://www.bristol.ac.uk/policybristol/policy-briefings/regulating-digitisation-of-critical-infrastructure-cyber-security-decisions-must-be-based-on-robust-evidence/

Contact the researchers

Dr Ola Michalec, Senior Research Associate at Bristol Cyber Security Research Group ola.michalec@bristol.ac.uk

National Cyber Security Centre
a part of GCHQ

RITICS

University of BRISTOL
Bristol Cyber Security Group