University of BRISTOL

PolicyBristol

Regulating digitisation of critical infrastructures: we need diverse experts to translate cyber security risks into the sector-specific contexts

Ola Michalec; Sveta Milyaeva; Awais Rashid (University of Bristol)

About the research

As digital innovations proliferate across critical infrastructure sectors, we begin to regulate them to ensure 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, uses the case study of the water sector in England to address how traditional environmental governance goals (water availability, affordability, sustainability, continuity of supply, public participation) compare against the cyber security ambitions. Our research traces how diverse experts collaborate on the NIS Directive. Practitioners like regulators, lawyers, senior managers, water engineers, IT security experts negotiate their interpretations of NIS to advance their respective priorities. Accessing the diversity of experiences and opinions is crucial so that the NIS could overcome the expertise asymmetry and allow non-technical experts to contribute towards agenda setting.

Policy implications

- The bottom-up involvement of experts in Operational Technologies, Safety Engineering and Environmental Politics experts is key to ensure a NIS implementation is inclusive of water governance issues.
- Security experts in Operational Technologies ought to train themselves to better communicate business benefits of security measures.
- We encourage the formation of sector-specific informal working groups for sharing information about NIS implementation, security maturity and evolving threats. Such groups ought to have clear terms of reference and scope to enable trustworthy information sharing.
- Following the translation of high-level NIS Directive into sector-specific assessments, regulators should reflect on residual spaces left unaccounted for by the emerging standard.

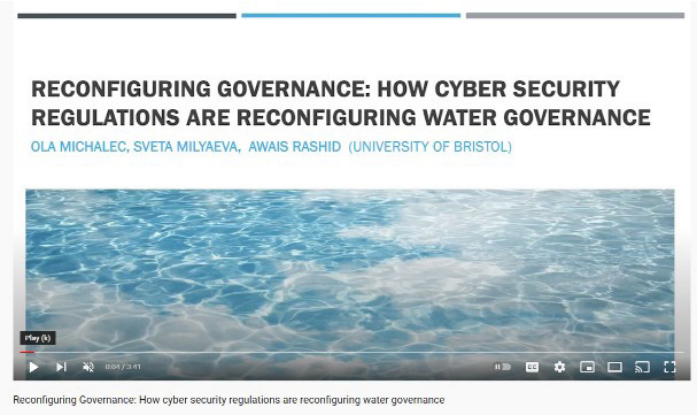
University of BRISTOL

PolicyBristol

Key findings

In the process of transposing the NIS Directive into the sectoral context, the regulations require interpretation by diverse expert communities. Translating the regulatoryscope to the sectoral landscape involves prioritizing some water governance goal over others. How is the water sector itself changing as a result of the 'digital water' agenda? We show that water practitioners typically translate typical cyber security concerns to the sectoral context in relation to water safety, availability and continuity of supply. However, we argue that this has not yet happened with the priorities of sustainability, affordability and public participation. Going forward, regulators will need to maintain a balance between competing governance priorities so that all of the strategic governance goals receive appropriate attention.

By forming new relationships between the regulators, manufacturers and water suppliers, and through creating new types of jobs or leveraging new funding mechanisms, the cyber security regulations have the potential to transform the water sector in both positive and negative ways. If collaborative relationships are not developed, and new types of jobs not created, then the alignment with all of the water governance priorities as a result of NIS implementation will be diminished.



Reconfiguring Governance: How cyber security regulations are reconfiguring water governance

Ola Michalec gives a short summary of the paper this briefing's recomendations are based on, *"Reconfiguring Governance: How Cyber Security Regulations Are Reconfiguring Water Governance."* Michalec, Ola, Sveta Milyaeva, and Awais Rashid. (2021). Watch the video on YouTube.

Further information

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, O., van der Linden, D., Milyaeva, S. and Rashid, A. (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/conference/soups2020/presentation/michalec

European Parliament (2016) Directive on Security of Network and Information Systems.

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

Contact the researchers

Dr Ola Michalec, 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