Policy Briefing 91: Sept 2020

University of BRISTOL

PolicyBristol

Regulating digitisation of critical infrastructure: cyber security decisions must be based on robust evidence

Ola Michalec; Dirk van der Linden; Sveta Milyaeva; Awais Rashid (University of Bristol)

About the research

Critical infrastructures (e.g. water, energy, transport) use Operational Technologies to provide their services. Operational Technologies are engineering equipment traditionally built for safety and resilience which, over the last few years, have been digitised and connected to the Internet. This creates new avenues for cyber security attacks: blackouts in power stations, pollution of water supply, hacked traffic signals.

The Network and Information Systems Security (NIS) directive aims to improve the baseline level of security across critical infrastructures. Since 2018, the European Union member states and the UK have been working on implementing it. NIS raises questions about defining scope, providing evidence or mobilising funding for digital innovation. Most importantly, critics have questioned whether it would become a tick-box exercise or lead to long-term improvements in security practices. In order to understand possible pathways of policy implementation, this research sought to understand how the Operational Technology expertise in critical infrastructure security is created. The notion of technical expertise is crucial to understand, as it is increasingly influencing the direction of policies like NIS, by providing advice and shaping the scope. We conducted interviews with 30 cyber security practitioners in the UK: including sectoral regulators, infrastructure operators, lawyers, consultants and training providers.

Image credit: Pexel

Policy implications

- Critical infrastructure operators should know about and protect themselves against threats which circumvent air-gapped systems. Check whether alternatives to air-gapping comply with safety standards.
- Regulatory bodies overseeing NIS should align the timescales of innovation funding and NIS improvement plans. When approving price reviews for network upgrades, seek robust evidence for the claims on the operational benefits of proposed innovations.
- All stakeholders should be aware of the differences between Operational Technology and Information Technology security solutions and priorities. Auditing needs to include both Operational and Information Technologies and the improvements ought to be tailored to each sector.
- Cybersecurity training providers should tie the training to employees' personal concerns to make it relatable and interesting. Do not rely on "awareness" alone - complement it with other training methods. Above all, place "awareness" in the usability context of daily work; i.e. plant supervisors have different concerns to admin staff.
- All stakeholders ought to seek development of skills in OT security through standardised training. The training should also include capabilities in the areas of human and social factors of technology. It is imperative that critical infrastructure practitioners implementing NIS do not compromise on other public values such as privacy, sustainability or equity.

Key findings

Without OT-specific expertise, security advice risks becoming a trope

- We introduce the term "security trope", to analyse common beliefs about best security practices which require a further level of detail before they can be successfully applied to the Operational Technology context. Since they are generic, they lead to the creation of advice which can be easily marketed at mass scale. As they are quite vague, they can appeal to professionals from diverse backgrounds. Our research discusses the issues that arise from the following four tropes:

  1. Network separation (air-gapping) means security.
  2. Innovation is inevitable, we can't shape the Internet of Things.
  3. Security solutions are the same across the sectors.
  4. Raising awareness leads to security.

NIS implementation faces a dilemma

- We found that NIS contrributed to the skills gap by generating a demand for expertise, which then was followed by unlocking investments in new staff. Critical infrastructure operators face two converging challenges:

  5. An increasing pressure to recruit Operational Technology (OT) experts: practitioners skilled in both engineering and computer sciences.
  6. Quality and expertise of OT professionals is inconsistent due to the varied routes into the career. Without recognised qualifications, employers face a challenge to identify capable candidates.

- As the question of NIS implementation is positioned in the centre of this dilemma, we risk that poorly evidenced and Operational Technology-inappropriate advice will be circulated to influence key security decisions. Furthermore, we argue that filling the skills gap is more than a matter of supply and demand in the OT security niche alone. As NIS pertains to services and resources essential to the society, it requires attention to public values such as privacy, sustainability, affordability.

Further reading

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).

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

Carr, M. and Tanczer, L.M. (2018) UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions. Journal of Cyber Policy, 3 (3): pp. 430–444.

Rashid, A.; Gardiner, J.; Green, B. and Craggs, B. (2019) Everything is awesome! or is it? Cyber security risks in critical infrastructure. In: International Conference on Critical Information Infrastructures Security, pp. 3–17. Springer.

Slayton, R. and Clark-Ginsberg, A. (2018) Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. Regulation & Governance, 12 (1): pp. 115–130.

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