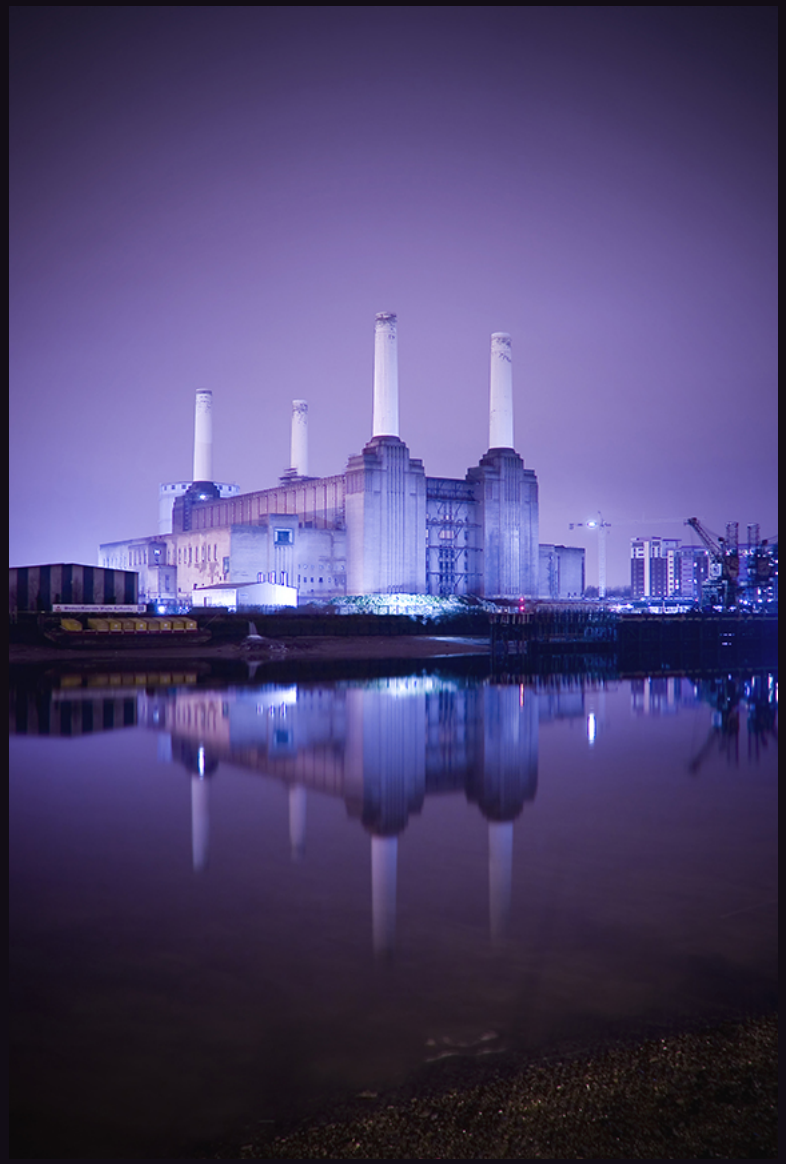
Industry Responses to the European Directive on Security of Network and Information Systems (NIS)

Dr Ola Michalec, Dr Sveta Milyaeva,
Dr Dirk van der Linden, Prof Awais Rashid

RITICS

University of BRISTOL
Bristol Cyber Security Group



Background

- Operational Technologies (OT): engineering equipment used in critical infrastructure sectors (e.g. water, energy, transport). Traditionally built for safety and resilience
- Now OT are becoming 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.
- Many questions arising: How to define the scope of the policy? How will NIS impact digital innovation? How to evidence OT are ‘secure enough’? How to ensure NIS won’t become a tick-box exercise?

RITICS

University of BRISTOL
Bristol Cyber Security Group

Research questions

1. How is the knowledge of OT security created?
2. How do CNI operators interpret and implement cyber security regulations?

Research design

Semi-structured interviews with 30 cyber security professionals in CNIs, consultancies, law firms, public sector
(October 2019-January 2020)

RITICS

University of BRISTOL
Bristol Cyber Security Group

Findings: how OT security expertise is created

1. Critical infrastructure operators face two converging challenges:

- An increasing pressure to recruit Operational Technology (OT) experts: practitioners skilled in both engineering and computer sciences.
- The 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.

2. We risk that poorly evidenced and Operational Technology-inappropriate advice will be circulated to influence key security decisions. We explore this risk by introducing the concept of ‘security tropes’.

3. Filling the “skills gap” is more than a matter of supply and demand in OT security niche alone. As NIS pertains to services essential to the society, it requires attention to public values.

RITICS

University of BRISTOL
Bristol Cyber Security Group

Findings: OT security tropes (example)

Trope: IIoT is inevitable

Analysis: The discourse of "inevitability" of innovation is consciously perpetuated by the IIoT manufacturers. CNI operators and regulators play an active role in deciding on the future of IIoT and other innovative technologies.

Risk to NIS: Regulations becoming a vehicle for implementing IIoT for its own sake, without concerning security and other public values.

NIS Recommendations for regulators: align the timescales of innovation funding, regular upgrades and NIS improvement plans. Seek robust evidence for the claims on the operational benefits of IIoT before approving funding.

Key messages

1. NIS requires to reconsider how OT security expertise is formed: who are the experts? What makes someone an expert? What if they disagree?

2. The pressure to implement security solutions combined with a sector-wide skills gap creates a fertile ground for developing security tropes.

3. The implementation of technical policies and standards is a two-way exchange: we need to pay attention to the debates and negotiation taking place before key decisions are made.

RITICS

University of BRISTOL
Bristol Cyber Security Group

Teaser: Four types of NIS implementation practices

	Compliance	Workaround	Going above and beyond policy remit	Negotiation
Security Example	Completing asset discovery as an essential basis for further cyber improvements	OT experts implementing their own security measures, using policy as a “sanity check”	Intelligence sharing through a working group set based on trust and shared terms of reference	Operators giving feedback to regulators: asking to improve IT security-biased language of policy documents
Insecurity example	Interpreting the scope of NIS to own advantage, while excluding key OT assets	Senior executives ignoring the need for improvements, based on their own interpretations of ‘appropriate and proportionate’ clause in NIS	Overreliance on the latest ‘buzzword’ technologies when basic knowledge about them is missing	Prioritizing business values over public values in policy interpretation (considering securing assets at the expense of customers’ privacy)

* Please see our full paper for more details!

Recommended reading:

Frey, S., Rashid, A., Zanutto, A., Busby, J. and Follis, K. (2016) On the Role of Latent Design Conditions in Cyber-Physical Systems Security. *2nd International Workshop on Software Engineering for Cyber Physical Systems*

Hallet, J., Larson, R. and Rashid, A. (2018) Mirror, Mirror, On the Wall: What are we Teaching Them All? Characterising the Focus of Cybersecurity Curricular Frameworks. *USENIX Workshop on Advances in Security Education.*

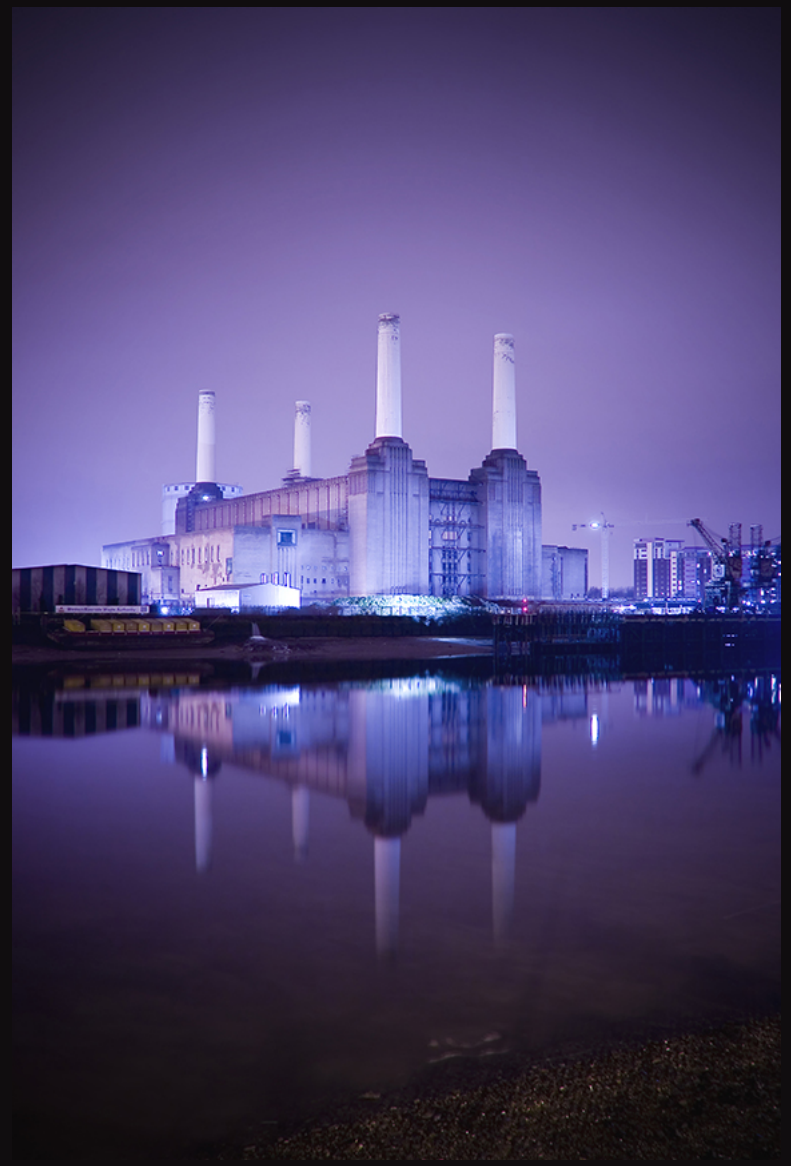
Rashid, A., Gardiner, J., Green, B. and Craggs, B (2019) Everything is Awesome! Or is it? Cyber Security Risks in Critical Infrastructure, *CRITIS*

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

RITICS

University of BRISTOL

Bristol Cyber Security Group



Thank you for your attention.
Any questions?

Email: ola.michalec@bristol.ac.uk

RITICS

University of BRISTOL
Bristol Cyber Security Group