Cyber security cultures in Critical National Infrastructures

Understanding policies, practices and sectoral differences

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

RITICS

University of BRISTOL
Bristol Cyber Security Group

University of BRISTOL
Bristol Cyber Security Group
RITICS
Ola.Michalec@bristol.ac.uk

Experts agree! Cyber security concerns go beyond “technical” issues

What does it mean in practice? What are the research questions, methods, collaborations we need to mobilise?

University of BRISTOL
Bristol Cyber Security Group
RITICS
Ola.Michalec@bristol.ac.uk

Four approaches to cyber security

1. Fixing broken objects, protecting objects from breaking (engineering, computer science)
2. Extension of political activities (international relations)
3. Usability, attitudes and behaviours (human factors, management)
4. Social practices enacted through the production of knowledge, evolving standards and diffusion of innovation (science and technology studies - STS)

(adapted from Dunn-Cavelty, 2018)

University of BRISTOL
Bristol Cyber Security Group
RITICS
Ola.Michalec@bristol.ac.uk

STS approach

Social practices

Production of knowledge

Evolution of standards and policies

Diffusion of innovation

(Shove and Trentmann, 2018)

University of BRISTOL
Bristol Cyber Security Group
RITICS
Ola.Michalec@bristol.ac.uk

Project Aim

To explore the co-evolution of cyber security expectations, technological innovations, formal policies and informal practices in the context of NIS implementation across the diverse CNI operators in the UK.

Research Question

How do evolving cyber security policies mutually shape CNIs' everyday security practices, business priorities and services they offer?

University of BRISTOL
Bristol Cyber Security Group
RITICS
Ola.Michalec@bristol.ac.uk

Research design

Stage 1: Semi-structured interviews with cyber security professionals in CNIs, consultancies, law firms, public sector (October 2019-January 2020)

Stage 2: Embedded case studies: ethnographic fieldwork in the offices of CNI organisations.
This includes: informal interviews, workshops and shadowing of CNI employees (January-June 2020)

LOOKING FOR COLLABORATORS!

(Yin, 2008; Neyland, 2008)

Ola.Michalec@bristol.ac.uk

University of BRISTOL
Bristol Cyber Security Group

RITICS

Policy landscape

- EU NIS directive (2016)
- UK NIS regulations (2018)
- UK Cyber Security Strategy (2016-2021)
- Overlaps with GDPR (2018)
- National Cyber Security Centre (2016)
- Role of the regulators (”Competent Authorities”)
- New public-private partnerships?
- Place-based scope: Local Resilience Forum (LRF), Warning and Advice Reporting Point (WARP)

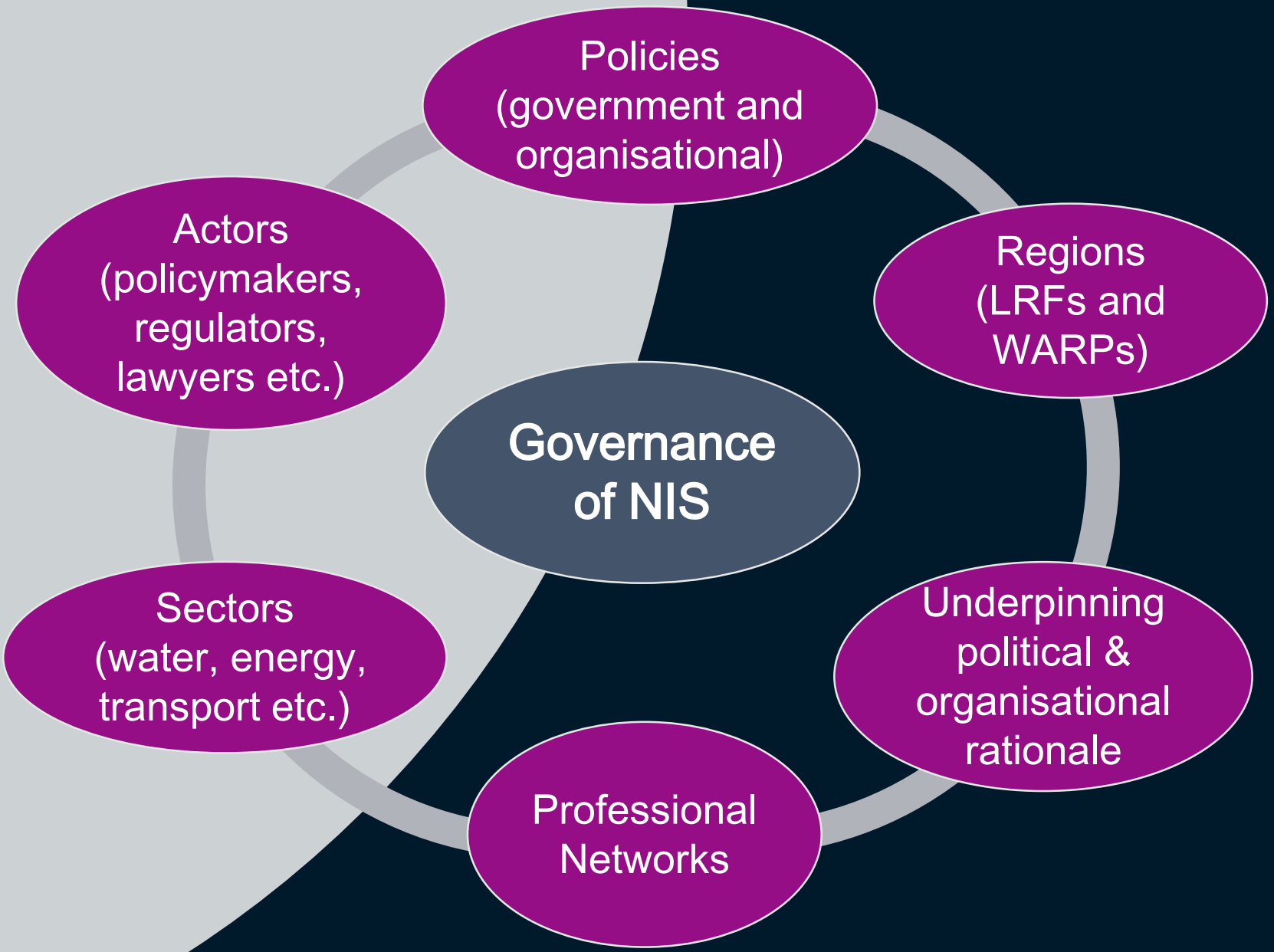
NIS progress to date

Organisations in scope submitted their self-assessment using NCSC’s Cyber Assessment Framework (CAF) to the relevant Competent Authorities. They’re currently discussing further development plans and third-party assessments.

Ola.Michalec@bristol.ac.uk

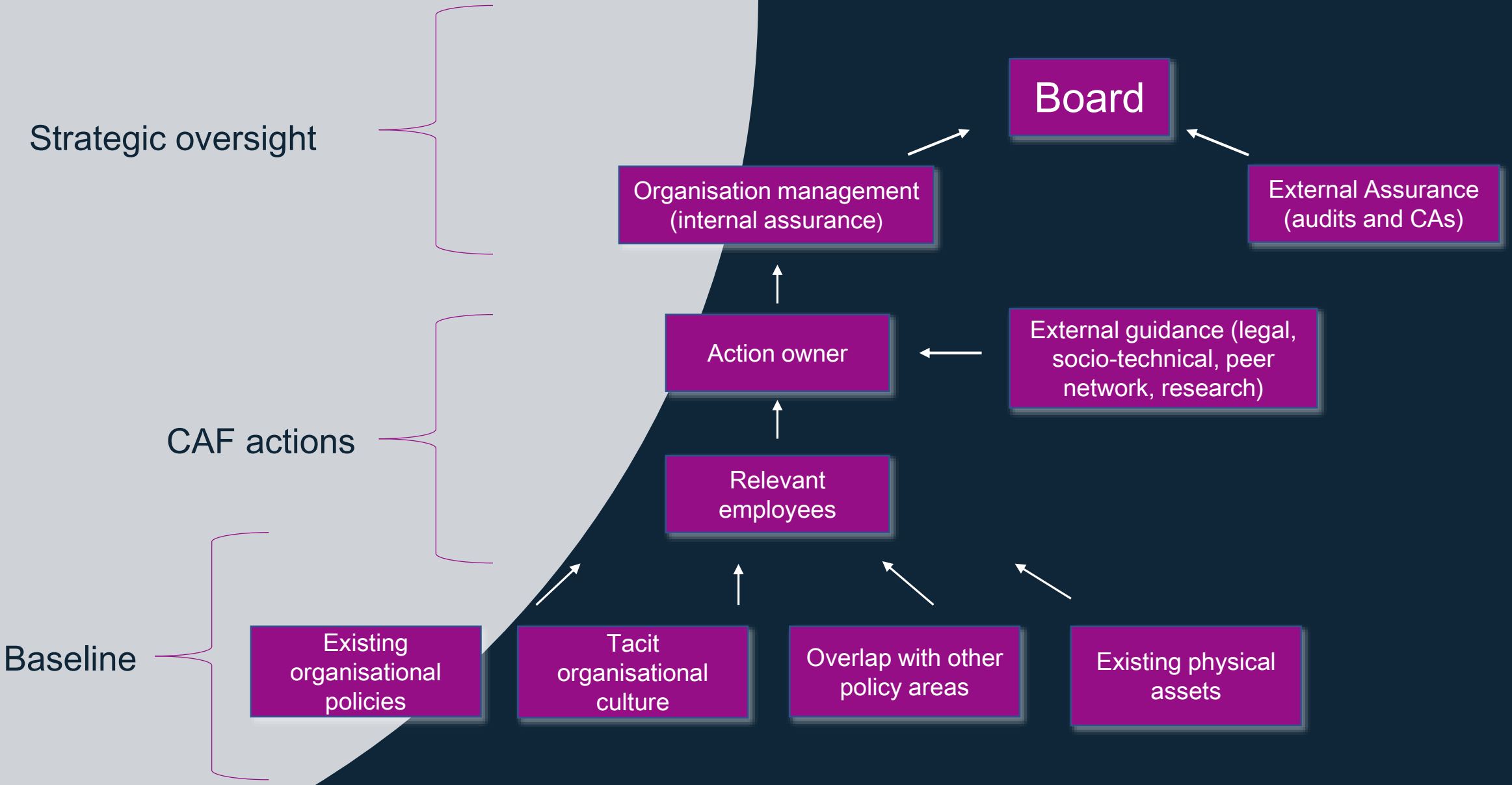
University of BRISTOL
Bristol Cyber Security Group

RITICS



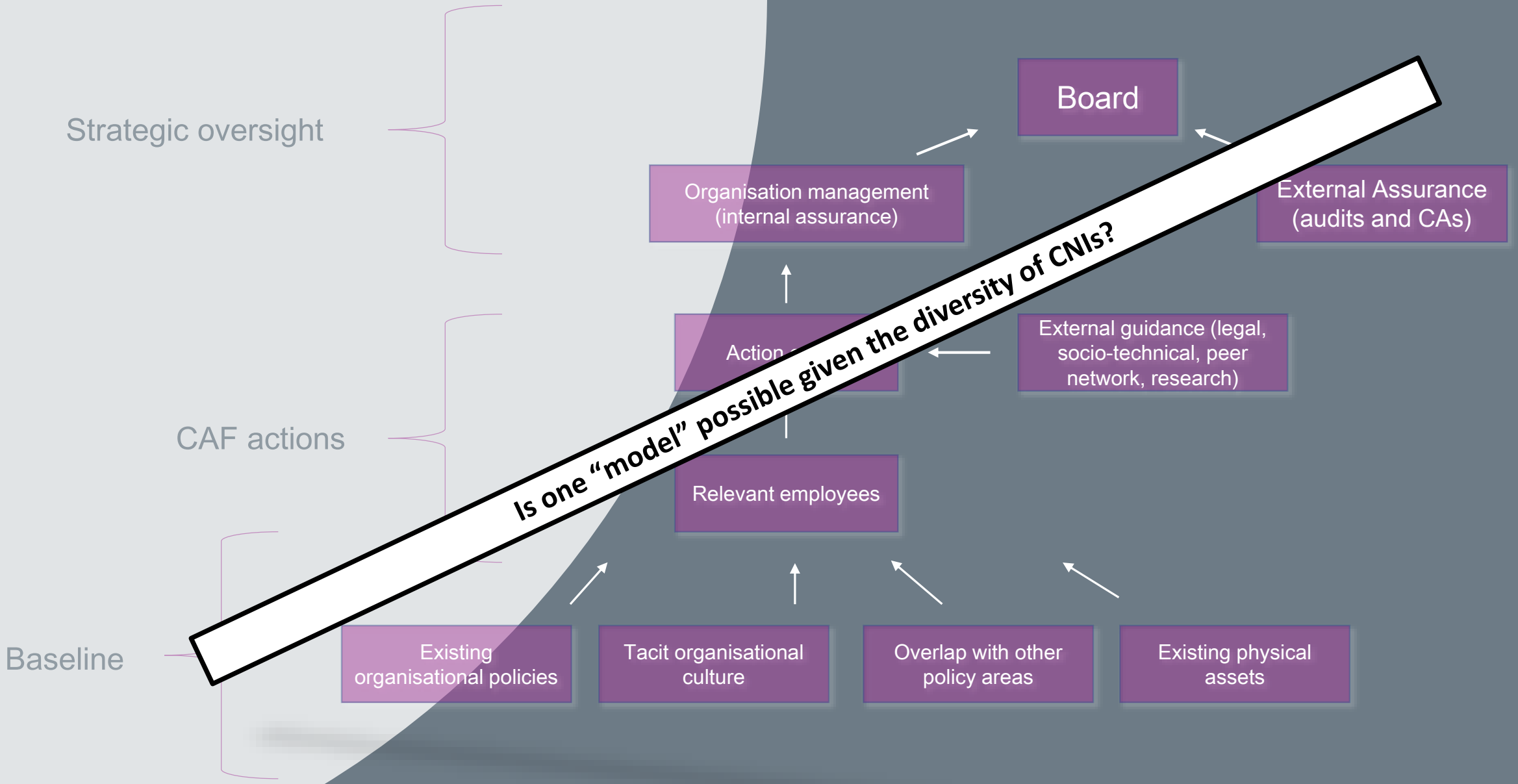
Model NIS implementation

Ola.Michalec@bristol.ac.uk



Model NIS implementation

Ola.Michalec@bristol.ac.uk

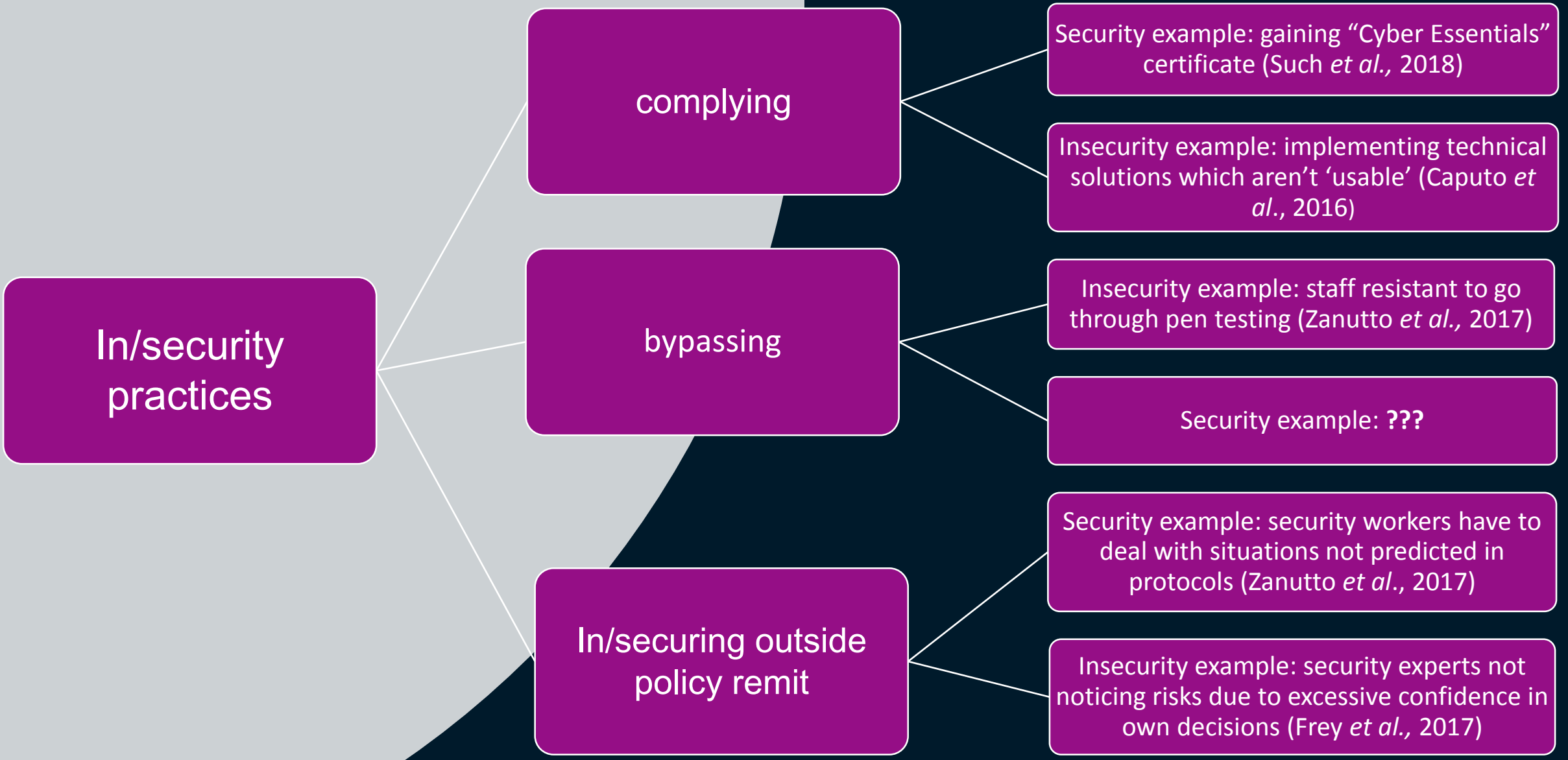


Early typology of practices

Ola.Michalec@bristol.ac.uk

University of BRISTOL
Bristol Cyber Security Group

RITICS



University of BRISTOL
Bristol Cyber Security Group
RITICS
Ola.Michalec@bristol.ac.uk

Summary

- We presented social science / STS perspective on cyber security
- We are tracing the ‘making of’ NIS directive
- We are interested in everyday security practices within diverse CNIs
- We will collect data through interviews (stage 1) and ethnographic fieldwork (stage 2)
- We are currently looking for participants and collaborators

University of BRISTOL
Bristol Cyber Security Group

RITICS

Ola.Michalec@bristol.ac.uk

References

Caputo, D.D., Pfleeger, S.L., Sasse, M.A., Ammann, P., Offutt, J. and Deng, L. (2016) Barriers to Usable Security? Three organizational case studies. *IEEE Computer and Reliability Societies*

Dunn-Cavelty, M. (2018) Cybersecurity Research Meets Science and Technology Studies, *Politics and Governance*, 6(2), p. 22-30

Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., Naqvi, S.A. (2017) The Good, The Bd and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. IEEE Transactions on Software Engineering

Neyland, D. (2008) Organisational Ethnography, Sage

Shove, E. and Trentmann, F. (2018) *Infrastructures in Practice: The Dynamics of Demand in Networked Societies.* Taylor and Francis

Such, J.M., Ciholas, P., Rashid, A., Vidler, J. and Seabrook, T. (2018) Basic Cyber Hygiene: Does it work?. Computer

Yin, R. (2008) *Case Study Research: Design and Methods*. Fourth Edition. Sage

Zanutto, A., Shreeve, B., Follis, K., Busby, J., Rashid, A. (2017) The Shadow Warriors: In the no man's land between industrial control systems and enterprise IT systems. Symposium on Usable Privacy and Security, July 12-14 2017, Santa Clara, California

Thank you for your attention

University of BRISTOL
Bristol Cyber Security Group

RITICS

Collaborate with us!

What? Hour-long face to face interviews (location and time chosen by participant)

When? Between October 2019 and January 2020

Who? People with professional experience of NIS (e.g. civil servants, consultants, lawyers, engineers, CEOs, Security Managers, regulators)

Why? We want to find out more about your experiences of NIS design, implementation and compliance.

Interested?

Email Ola.Michalec@bristol.ac.uk for more information
Twitter @BristolCyberSec