What’s next for the NIS Regulations?

Findings from RITICS Fellowship

Dr Ola Michalec
Bristol Cyber Security Group

National Cyber Security Centre
a part of GCHQ

University of BRISTOL
Bristol Cyber Security Group

RITICS
RESEARCH INSTITUTE IN TRUSTWORTHY INTER-CONNECTED CYBER-PHYSICAL SYSTEMS

Table of Contents

1. Introduction

1.1. Background

As modern computing technologies are introduced to critical infrastructure sectors, they become regulated to ensure the reliable and safe delivery of essential services like water, energy, or transport. Cyber security governance is a prime example of such efforts, with the Network and Information Systems Security (NIS) Directive (European Commission, 2016) implemented across the EU in 2016 and then transposed to the UK context as NIS Regulations in 2018 (DCMS, 2018). NIS is a novel regulatory response to the increased interconnection of industrial computers to the internet.

Over the past five years, the UK government designated the Operators of Essential Services (OES) and Digital Service Providers (DSP) falling into the scope. Through the series of stakeholder consultations, thresholds for incident reporting and principles of good security governance have been identified through the creation of the Cyber Assessment Framework – CAF (NCSC, 2022). The practitioners working on NIS in the UK continuously emphasised the need for understanding best practice specific to Operational Technologies (OT) as well as furthering efforts to harmonise security and safety requirements.

NIS Regulations are now at a critical juncture. With the proposals to radically extend the scope of NIS in the EU and the renewed attention to critical infrastructure protection in mainstream media due to the war in Ukraine, the future of NIS in the UK is yet to be decided.

In order to determine the most favourable pathway for the future of critical infrastructure security governance, we first need to understand the current regulation implementation landscape. **This report, based on three years of research funded by the Research Institute in Trustworthy Interconnected Cyber-Physical Systems (RITICS), outlines a series of collaborative governance practices, remaining challenges to NIS and CAF implementation, and recommends a set of actions for policy and research**.

1.2. Research Design

This report draws on over three years of qualitative research and active engagement in the network on professionals working on implementation of the NIS Regulations in the UK. In particular, the document summarises research findings from the projects funded by the Research Institute on Trustworthy Interconnected Cyber-physical Systems (RITICS): 1) How many shades of NIS? Understanding organisational cyber security cultures and sectoral differences (please see the bibliography to access peer-reviewed outputs this report draws on); 2) RITICS Fellowship: What's next for the NIS Directive? Extending the community of interest to better understand the "Indicators of Good Practice".

The research data consists of interviews with 30 participants conducted between October 2019-January 2020 and focus groups with 36 participants that took place between February-March 2022. Research participants were UK-based stakeholders with experience in the NIS Regulations and/or cyber security of critical infrastructures.

In addition, the author was embedded in expert networks (such as RITICS and the NCSC Industrial Control Systems Community of Interest) through active participation in events and contribution to ongoing work on security guidance.

1.3. The NIS Regulations in the UK

NIS originated as a high-level supranational directive ratified by the European Parliament in 2016 (European Commission, 2016). Since then, it has been transposed to the EU Member States and the United Kingdom as NIS *Regulations* (DCMS, 2018). In the United Kingdom, the implementation of NIS follows the principles of 'appropriateness and proportionality' (Michels and Walden, 2018), which necessitates careful deliberation over designation of the operators falling under the purview of regulations, thresholds of incident reporting and maximum penalties. NIS is known as 'principles-based regulation', meaning that critical infrastructure operators work towards meeting the governmental objectives without specification how to achieve such goals (Michels and Walden, 2018). The government's reasoning behind this move is to avoid 'box ticking' style of compliance and contextualise risk management.

The implementation procedures in the United Kingdom begin with a self-assessment stage (known as the Cyber Assessment Framework - CAF; NCSC, 2022). The Cyber Assessment Framework is the key operational document pertaining to the question of cyber security risk management of critical infrastructures in the United Kingdom. Fourteen principles of the Cyber Assessment Framework are set out as so-called 'Indicators of Good Practice' - IGPs (NCSC, 2022), or recommended outcomes of security improvements rather than specification *how* to improve cyber security. Each of the 14 outcomes is self-assessed according to a three-grade red/amber/green (RAG) scale as either 'fully achieved', 'partially achieved' or 'not achieved'. Following the completion of self-assessments, operators and regulators draw agreements on the improvement plans, and conduct external audits (Michalec et al., 2020; Wallis and Johnson, 2020).

1.4. Who should read this report?

This report is relevant to the stakeholders working on the NIS Regulations in the UK and across the EU. The target audiences include Competent Authorities, Operators of Essential Services, Digital Service Providers, policymakers setting the strategic direction of cyber security in the government, standardisation practitioners, researchers of critical infrastructures security, and security consultants.

1.5. Summary of findings and recommendations

1.5.1. Research findings

The report 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. Successful implementation of NIS involves a variety of **collaborations**, e.g., across managers and technical professionals, across the operators, and across safety and security experts, as shown on the figure below.

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. Going forward, we **recommend** that NIS stakeholders encourage collaborative practices to implement NIS and advance security at a societal level, rather than working at organisational level only.

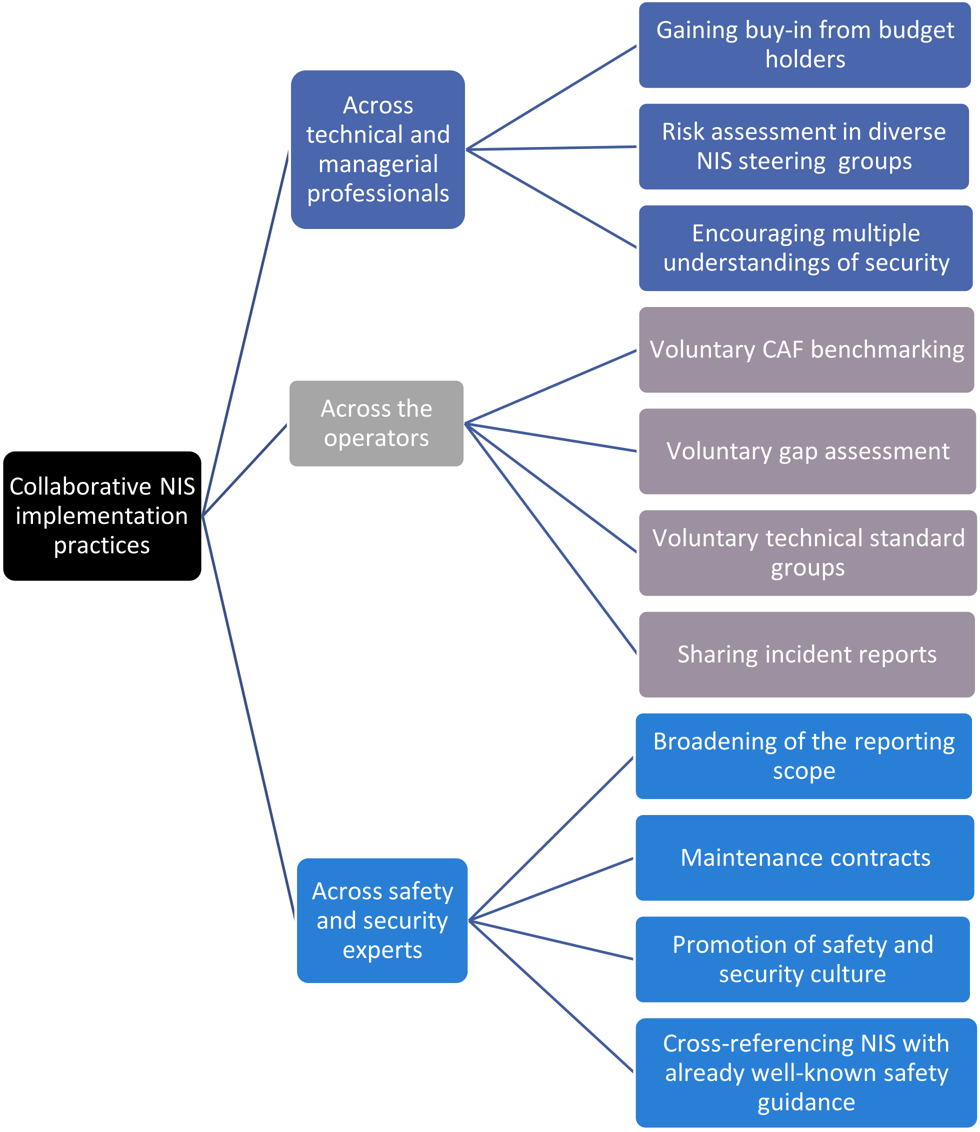
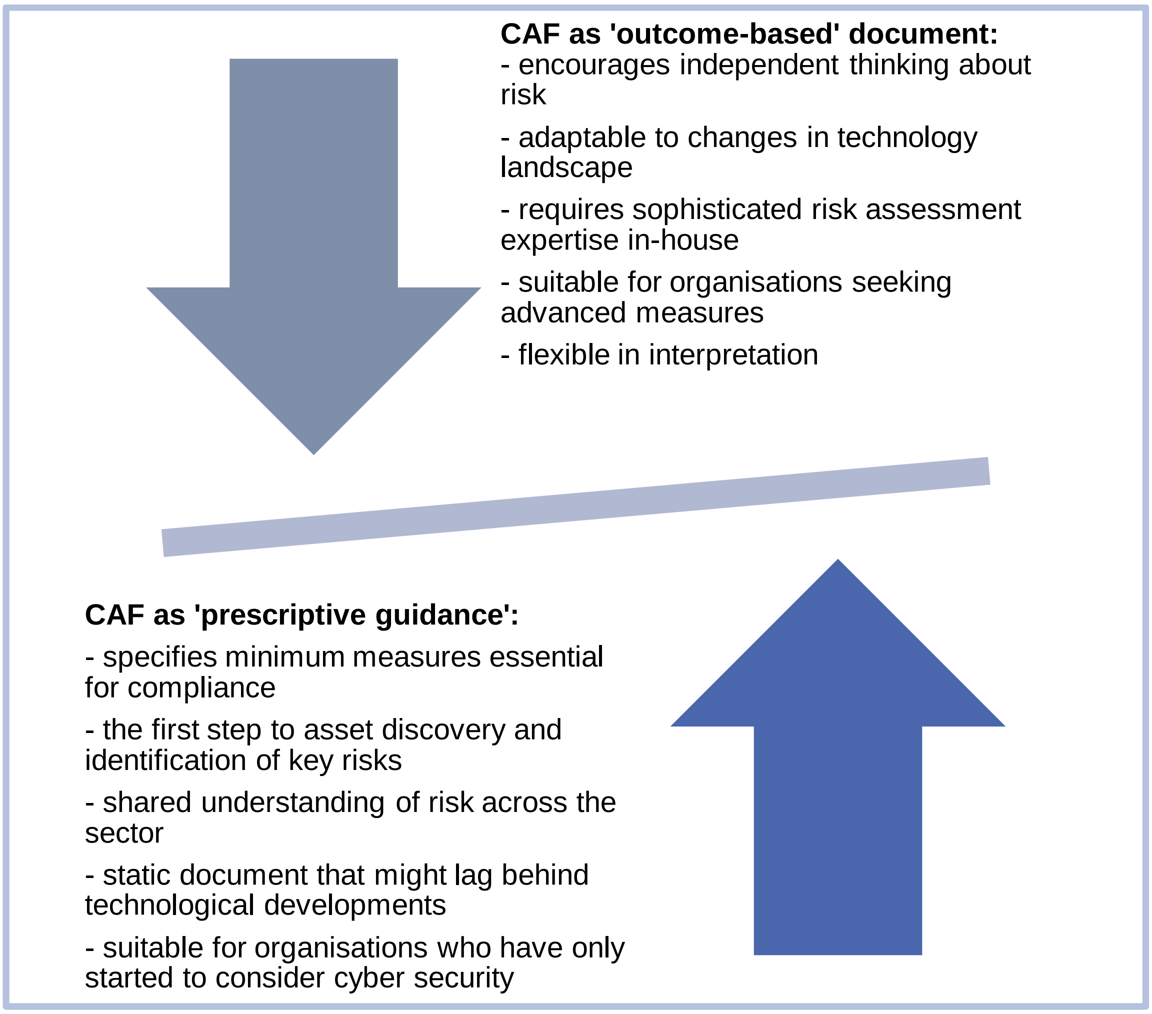

Collaborative NIS implementation practices
Across technical and managerial professionals
Gaining buy-in from budget holders
Risk assessment in diverse NIS steering groups
Encouraging multiple understandings of security
Across the operators
Voluntary CAF benchmarking
Voluntary gap assessment
Voluntary technical standard groups
Sharing incident reports
Across safety and security experts
Broadening of the reporting scope
Maintenance contracts
Promotion of safety and security culture
Cross-referencing NIS with already well-known safety guidance

***Figure 1**. Collaborative NIS implementation practices*

The report analysed the implementation of Cyber Assessment Framework (CAF). CAF 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 **conclude** that outcomes-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.



CAF as 'outcome-based' document:

- encourages independent thinking about risk
- adaptable to changes in technology landscape
- requires sophisticated risk assessment expertise in-house
- suitable for organisations seeking advanced measures
- flexible in interpretation

CAF as 'prescriptive guidance':

- specifies minimum measures essential for compliance
- the first step to asset discovery and identification of key risks
- shared understanding of risk across the sector
- static document that might lag behind technological developments
- suitable for organisations who have only started to consider cyber security

Figure 2. *The CAF Paradox: designed as an outcomes-based document, occasionally implemented as prescriptive guidance.*

1.5.2. High level policy recommendations

Policy Recommendations:

- The UK Government ought to balance between the proposed broadening of the scope and advancing maturity of safety-critical systems.
- The UK Government should share the strategic directions with regards to the future of NIS to enable alignment with similar initiatives.
- The UK Government ought to respond to the dilemma between achieving a common baseline and proactive risk management.
- All stakeholders should consider the cascading effects on small operators that currently do not fall under scope, especially as interoperability and digitalisation initiatives are under way.

1.5.3. NIS Research Gaps

Future NIS research gaps:

- A systematic comparison between the sectors: How are regulators utilising CAF? Which sectors are treating it as compliance tool, and which sectors are using it as a risk assessment tool?
- Which requirements (if any) should be seen as an essential security baseline?
- A horizon scan on the state of cyber security maturity regarding emerging technologies, processes and organisations that are likely to fall within the scope of NIS in 5-10 years' time.

2. Collaborative NIS implementation practices

2.1. Practices of cross-organisational collaboration

Stakeholders engaged in the implementation of the NIS Regulations emphasised the need for collaboration to build capability across the whole industry rather than solely at an organisational level (Michalec *et al.,* 2021). Successful collaborations have occurred across organisations (e.g., multiple operators within a sector) and professional cultures (e.g., safety and security experts). By building mutual trust and collegiality, NIS practitioners were able to translate their professional differences and work towards a common goal. This report will outline instances of successful collaborations and highlight remaining challenges to working together in an effective manner.

In terms of fruitful collaborations, participants associated them with small group size and informality that was conducive to trust building. They also took time to establish terms of reference, and processes for anonymisation and network building. Finally, the meetings of successful voluntary groups were led by a respected senior facilitator who would dare to ask the uncomfortable questions and ensure a fair 'give and take' in the room (i.e., by challenging the attendees who were reluctant to share information and only recorded notes). However, collaborating on cyber security governance via informal networks comes at a price. Ultimately, voluntary networks are fragile, as they lack formal recognition and rely on the good will of the stakeholders involved.

Below we outline cross-organisational collaborative practices deemed helpful by the NIS stakeholders.

Voluntary benchmarking for the Cyber Assessment Framework (CAF)
All Operators of Essential Services (OES) in one of the sectors gathered to share their early versions of CAF self-assessments, current cyber security maturity and levels of investment made. It facilitated submission of more accurate and realistic CAF documents (Michalec et al., 2021).

Voluntary sector-wide gap assessment
Operators in one of the sectors formed a voluntary working group to identify collective gaps in cyber security knowledge and practice. They used that knowledge to build a case for support from the government. The working group also organised knowledge sharing events between mature companies and those with low level of cyber security capability. Finally, the group discussed the instances where ‘best practice’ advice differs between the operators (Michalec et al., 2021).

Voluntary bottom-up working groups creating sector-specific standard
A group of engineers in one of the sectors established a working group to create a secure telemetry standard. They argued that their initiative is relevant to the sectoral context and goes above and beyond the ‘vague’ language of CAF (Michalec et al., 2020).

Sharing incident reports across sectors
The regulators highlighted the need for cross-sectoral learning between organisations at different stages of digitalisation. Incidents and the associated responses ought to be thoroughly documented and shared through reports and meetings with representatives of other sectors.

2.2. Practices of harmonising safety and security

Although cyber security is a novel requirement for critical infrastructure practitioners, it holds multiple parallels with a well-known paradigm of safety in engineering (Michalec et al., 2022). Harmonisation of safety and security is seen as favourable as it uses the language and examples that are already known to OT practitioners.

Broadening of the reporting scope
Regulators in one of the sectors required safety accidents and security incidents to be reported through the same process. The decision was justified as a move to de-stigmatise being affected by security incidents and encourage honest reporting (Michalec et al., 2021).

Maintenance contracts between third party suppliers and operators
Safety engineers recommend translating their well-established practices to the world of Operational Technology (OT) Security. For example, maintenance contracts could be drawn to assign roles and responsibilities for security over time. However, maintenance contracts still require the operators to understand the supply chain all the way down. Supply chain contracts should not replace organisational knowledge about the assets and security risks (Topping et al., 2021).

Alignment between security & safety culture
Research informants emphasised the need for cultural acceptability of the NIS Regulations among the safety engineers who have been working on the OT systems over the last several decades. Security practices, therefore, need to align with day-to-day demonstrations of 'safety culture' - collective norms, behaviours and institutional enablers proven to provide safe deliver of essential services. Examples of 'safety culture' practices are: thorough reporting of accidents, looking after colleagues, continuous assessment against major risks, root cause analysis (Common Safety Methods, the EU Agency for Railways, n.d.; Michalec et al., 2022).

Cross-referencing NIS with already known safety regulations
Increasing cultural acceptability of NIS can also achieved by demonstrating that the expectations and practices from NIS align with already existing and familiar safety regulations (e.g. Common Safety Methods, the EU Agency for Railways, n.d.).

2.3. Collaborative practices between diverse experts

Cyber security of critical infrastructures involves collaborations between practitioners with expertise in machines, software, behaviours, and broader sectoral contexts.

The following instances ensured relevance of NIS to both day-to-day and strategic goals of the operators:

Diverse teams working on risk management
Some operators assembled diverse teams to conduct risk management for NIS (e.g., by setting a NIS Steering Group). They emphasised the importance of forming a team of workers who trust each other. Teams would be diverse in their make-up, involving engineers, managers, and human factors practitioners. This improved the understanding risk management as an inherently anticipatory and socio-technical practice rather than something one can reduce to calculations (Michalec et al, 2022).

Technical practitioners gaining buy-in from senior management
OT practitioners emphasised the importance of communicating how security serves the strategic goals of their organisation. This meant that security was framed as a domain supporting operational functions of the business. Cyber security experts are now moving away from threat-based narratives (Michalec et al., 2022).

Encouraging multiple understandings of security in the early stages of NIS
Early stages of scoping the remit of NIS involved mobilising diverse expertise ranging from the EU officials, the UK regulators, the UK senior civil servants, Industrial Control Systems (ICS) manufacturers, software vendors, and operators. The diversity of inputs

enabled an improved designation of the ‘essential services’ and appropriate scoping of the regulations. Cyber security was understood in multiple ways, i.e., protection of residents, protection of environment, protection of company, protection of state interests and, finally, generation of market demand for innovation (Michalec et al., 2021).

3. Challenges for collaborative implementation of NIS

3.1. Challenges to safety-security harmonisation

The logics of risk assessment differ across safety and security
While the probability of safety failures is well grounded in historical records and components testing, security incidents are a function of anticipating malicious behaviours and relying on sparse and classified historical data, which does not lend itself easily to the logics of probabilistic prediction (Michalec et al., 2022).

Lack of a systematic and integrated root cause analysis for safety and security
The causes of security and safety incidents should be differentiated and thoroughly reported as 'lessons' for the future.

Encouraging sharing information for ongoing threats
Differentiating between a potential threat, a near miss and an incident is not always clear-cut and has political consequences with regards to taking responsibility for damages and penalties for non-compliance. Meanwhile, although incidents require reporting, near-misses and threats do not. Encouraging reporting of the ongoing threats to the regulator (or information sharing point, as relevant) will improve building data for future modelling of cyber security risks (Michalec et al., 2022)..

Here, a common counterargument is that operators might be afraid to share the threats and vulnerabilities as it might expose their gaps in front of the regulators who penalise them. However, if cyber security is to be understood as a societal good, there is a strong case for the regulators (or information sharing exchanges) knowing about the gaps. As we are collectively working to build cyber security capability, the focus of threat reporting would be on gap analysis and mitigation rather than penalising operators.

Prescriptive thinking in engineering
While (some) regulators promote CAF as an outcomes-based document, i.e., a subjective tool that encourages independent risk thinking, some engineers working on ICS on a day-to-day basis, still expect prescriptive standards that simply outline a list of measures of apply. Prescriptive standards mandating a list of baseline improvements are suitable for organisations which are commencing their cyber security journey (Michalec et al., 2022).

3.2 Challenges to collaboration between experts

Focusing on compliance rather than managing risks
CAF audits can hamper organisational reflexivity. NIS Regulations run the risk of creating a position where a lawyer defines what cyber security incident is, rather than a security practitioner. This would prioritise compliance over risk management, as operators would be discouraged from dealing with and reporting on difficult issues.

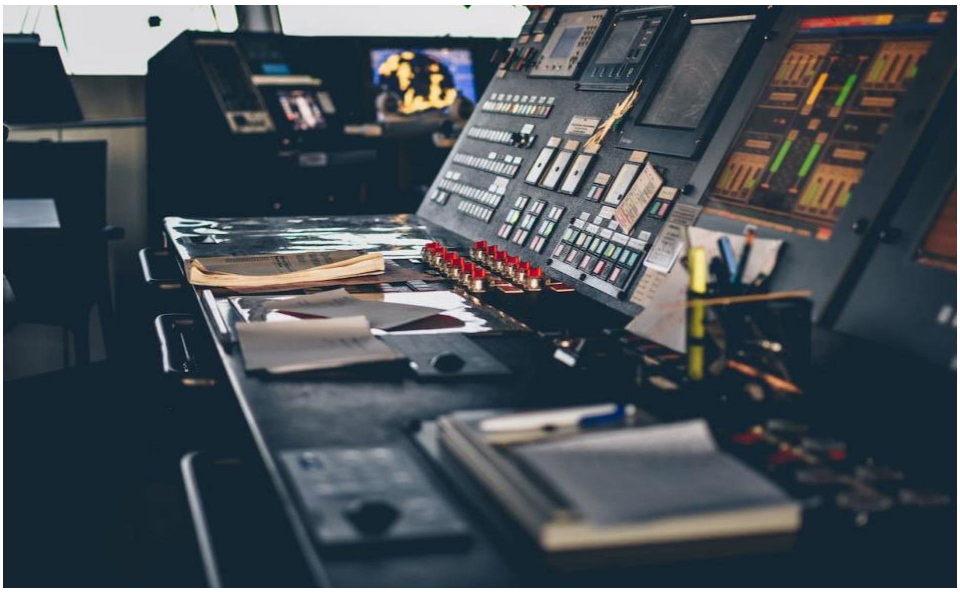
Conflicts between OT and IT teams
Collaborations including diverse teams are inherently challenging due to a potential for cultural clashes. Cyber security involves a power struggle as workers may clash over access management, maintenance regimes, budgets, and routes to leadership.

3.3. Other NIS Challenges

Low maturity of asset management
Our participants noted that cyber security decisions are rarely based on systematic assessments of asset criticality. In particular, operators with numerous geographically distributed assets found it challenging to account for their equipment. Asset discovery is further complicated by the relationships between the operators and Original Equipment Manufacturers (OEMs) who are typically undertaking maintenance duties. In some cases, operators were solely reliant on the third-party maintainers and had little awareness of their own asset inventories.

Presence of incorrect OT tropes
During the period of our research, we observed the presence of generalisations about the best OT security measures, i.e., ‘air gapping guarantees security’, ‘IIoT is inevitable and we can’t influence its security’, ‘security solutions are the same across the sectors’, or ‘raising awareness always leads to security’. The above statements are poorly evidenced and not always appropriate to the OT context. However, due to their popularity there is a risk that such generic advice can circulate to influence decisions. There is a need for contextualised cyber security guidance for OT environments (Michalec et al., 2020).

Overreliance on the latest ‘buzzwords’ and trends in technology
Our research found a worrying trend, where operators rely on the latest hypes in innovations (i.e., applying machine learning for anomaly detection). This is happening at the expense of basic knowledge about assets and organisational priorities. There is a tendency to treat automated solutions as a one-off purchase. Meanwhile, cyber security is a matter of ongoing maintenance, with human decisions being essential to the correct functioning of the ICS (Michalec et al., 2020)



4. CAF Paradox

4.1. On tensions between outcomes-based and prescriptive regulations

The UK NIS Regulations, together with the introduction of the Cyber Assessment Framework (CAF) are welcome changes to the critical infrastructure sectors. CAF is a much needed and well-timed step to improve security of the operators of the essential services. As a direct result of CAF, critical infrastructure stakeholders reconsidered their digitalisation programmes and hired or trained security practitioners with a dual expertise in IT and OT systems. Together, they commenced the long process of identifying good cyber security practices and applying them to the context of their workplaces.

Our participants have noted that CAF has been used in a variety of ways, on occasions contradictory to its formal purpose. Despite being designed as an outcome-based framework to guide independent risk assessment and discourage ‘box ticking’, in some cases, CAF has been used as a prescriptive document. We call this phenomenon ‘the CAF paradox’.

Our analysis highlights that the prescriptive approach to CAF can be justifiable in some cases. While the compliance-oriented and prescriptive approach does not advance operators to sophisticated levels of cyber security protection, it helps them to arrive at a common understanding of major risks and implement basic controls. Stakeholders in critical infrastructure sectors are culturally acclimatised to prescriptive standards and should not be expected to perform advanced risk management if they do not have asset discovery programs in the first place. As such, implementing outcomes-based regulations requires anticipatory exercises and in-depth knowledge of organisational assets, threat landscape and contextual risks.

4.2. CAF Recommendations

We recommend the following practices to improve the implementation of the Cyber Assessment framework:

- Competent Authorities to clearly communicate the aim of self-assessments to the operators as well as the executive boards (i.e., CAF as a way to identify gaps, manage risks and agree on implementation plans). As a result, operators will not under pressure to achieve ‘green’ Indicators of Good Practice at all costs.
- Competent Authorities to emphasise the need to evidence operators’ cyber security journey over time. The evolution of cyber security posture over time is more important than self-assessing an outcome as ‘green’.
- Competent Authorities to highlight the need to continuous maintenance of ‘green’ CAF status. Operators ought to include CAF cyber security measures as their business-as-usual and prepare a long-term program of maintaining good cyber security outcomes
- In the future, CAF inspections should move towards the analysis of emerging risks, gaps and evaluating operators’ responses over time.

5. NIS2

5.1. NIS2 in the EU and the UK

The second iteration of NIS Directive, namely NIS2, has been discussed at the European Union level over the past several months. In May 2021, the EU legislators reached a provisional agreement on the draft of the NIS2 Directive. In the coming months, the EU Parliament will vote on the adoption of NIS2.

The current proposals recommend the following changes (European Commission, 2021):

- To expand the scope by adding new sectors (telecoms, social media platforms, public administration, data centres, wastewater, waste management, manufacturing of critical products, food, space, postal and courier services).
- To remove the distinction between the Operators of Essential Services and Digital Service Providers.
- To address the security of ICT supply chain.
- To create novel requirements for incident reporting, vulnerability disclosure and administrative sanctions to improve alignment across member states and enable more stringent supervision.
- To increase trust by sharing more information and setting rules for large-scale incident response.

In short, the most significant difference is scope expansion, beyond what's traditionally considered Operational Technologies (OT) and safety-critical systems. If the UK Government is to follow suit, the main challenge will be balancing between improving security of the sectors new to NIS (many of them using IT systems rather than OT), while advancing the maturity of safety-critical OT systems. As we show throughout this report and previous publications (Michalec et al., 2020, 2021, 2022), the successful implementation of NIS so far has relied on translation between 'best practices' from the realm of safety to security.

Over summer 2022, the UK Government consulted on "future-proofing the UK NIS Regulations" (DCMS, 2022). The consultation included proposals on the following changes:

- To expand the scope of Digital Service Providers to 'managed services' (e.g., security monitoring, managed network services or the outsourcing of business processes) to improve the security of supply chains.
- To provide ministers with powers to make policy updates to NIS Regulations without changing the overall remit of the Regulations to become more responsive to the dynamic landscape of innovations, threats, and geopolitics.
- To create powers that would allow the government to change the scope of the NIS Regulations to include new sectors.
- To create a new power to designate 'critical' suppliers or services on which the existing 'essential operators' and 'digital service providers' depend.
- To expand the incident reporting requirements.
- To transfer the full costs incurred by competent authorities for regulating NIS from the taxpayer onto the organisations in scope by creating a more flexible

model that allows them to raise fees and recover costs for relevant NIS activities.

Although the UK had decided to implement the first iteration of EU NIS Directive after Brexit, it is unclear what the future of critical infrastructure security governance will be in the long term.

5.2. Policy recommendations for the future of NIS in the UK

We recommend the following actions:

- The UK Government ought to balance between the proposed broadening of the scope (DCMS, 2022) and advancing maturity of safety-critical systems.
- The UK Government should share the strategic directions with regards to the future of NIS to enable alignment with similar initiatives (e.g., standardisation of Energy Smart Appliances (BEIS, 2022).
- The UK Government ought to respond to the dilemma between achieving a common baseline and proactive 'outcomes-based' risk management. A consideration of two-tier regulatory measures ought to take place to address this dilemma.
- All stakeholders should consider the cascading effects on small operators that currently do not fall under scope, especially as interoperability and digitalisation initiatives are under way (BEIS, 2022).

Above all, future UK Government activities ought to prioritise communicating clarity in the strategic direction. We need a timely response to the EU proposals on NIS2 to enable harmonisation at the international level and cross-referencing NIS to upcoming standards (e.g., consumer IoT security) and sectoral security initiatives (e.g., Energy Smart Appliances). We can expect renewed discussions on scope, incident thresholds and the notion of 'appropriateness and proportionality'.

6. Research needs

The report identifies the three key knowledge gaps in the area of NIS implementation. We suggest the following prompts are utilised during future consultations and internal projects of research teams at DCMS or the NCSC.

Research need #1: A systematic CAF comparison between the sectors. How are different regulators utilising CAF? Which sectors are treating it as compliance tool, and which sectors are using it as a risk assessment tool?

Research need #2: Towards a shared understanding of basic cyber security measures in CNI. Which requirements (if any) should be seen as an essential security baseline? How should they be operationalised?

Research need #3: A horizon scan on the state of cyber security maturity regarding emerging technologies, processes and organisations that are likely to fall within the scope of NIS (or other cyber security policy initiatives) in 5-10 years' time.

7. Security for what? High level reflections

Can critical infrastructures, with their paramount concern about safety, adjust to the new reality brought about by digitalisation? Modernisation of legacy systems brings about the need to reconsider traditional paradigms in both engineering and computing in order to successfully integrate them (Hoolohan, et al., 2021). The NIS Regulations aim to advance the management of risks to critical infrastructures. At the same time, they facilitate the UK Government's agenda to adopt digital innovations in novel context in order to become a leader in a competitive global market and create jobs for the future generations (Cabinet Office, 2022). As we're at the cusp of extending cyber security governance to new domains (DCMS, 2022; Home Office, 2022), we ought to reflect on the past five years of NIS implementation in the UK.

First, we need to analyse the unfolding consequences of digital transformation in critical infrastructures. Are modern computing technologies in the OT environments living up to their promises? What are they augmenting or replacing? What is happening to legacy technologies and expertise? How to best account for critical infrastructures modernising at a variety of timescales and with diverse technologies?

Second, the costs of cyber security improvements and NIS implementation ought to be carefully monitored. What happens if security is deemed too expensive by the operators? Could cyber security measures impact the affordability of essential services?

Third, we ought to consider how to align the timescales of innovation adoption and security regulations. How to prevent releasing a whole generation of insecure infrastructures? This is particularly relevant to infrastructural improvements that citizens are interacting with, e.g., smart home appliances, electric vehicle chargers.

Through the means of qualitative research engaging experts on critical infrastructure security, this report highlighted successful NIS implementation practices as well as the remaining challenges. In particular, this work emphasises the value of collaboration across organisations and professional domains. Going forward, the report brings attention to the uncertain future of critical infrastructure security governance and recommends actions for the UK policymakers to improve the clarity of their strategic direction.

Acknowledgements

I would like to thank the Research Institute for Trustworthy Interconnected Cyber-Physical Systems and the National Cyber Security Centre for sponsoring this Fellowship.

I would like to also extend my gratitude to cyber security experts who shared their insights with us during workshops and interviews.

Finally, many thanks to co-authors (Prof Awais Rashid, Dr Sveta Milyaeva, Colin Topping, Dr Dirk van der Linden, Dr Andrew Dwyer, and Dr Barney Craggs) as well as to Sharad Agarwal, Anthony Mazeli, Dr Joe Gardiner, Dr Alma Oracevic, Khadiza Laskor, and Trevor Jones for event facilitation and assistance with data analysis.

References

1. Cabinet Office (2022). National Cyber Strategy 2022. Policy Paper. Available at: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

2. Department for Business, Energy, and Industrial Strategy (2022). Delivering a smart and secure electricity system: the interoperability and cyber security of energy smart appliances and remote load control. Available at: https://www.gov.uk/government/consultations/delivering-a-smart-and-secure-electricity-system-the-interoperability-and-cyber-security-of-energy-smart-appliances-and-remote-load-control

3. Department for Digital, Culture, Media, and Sport (2018). The NIS Regulations 2018. Available at: https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

4. Department for Digital, Culture, Media and Sport (2022). Proposal for legislation to improve the UK's cyber resilience. Consultation. Available at: https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience

5. European Commission (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

6. European Commission (2022). The NIS2 Directive: A high common level of cybersecurity in the EU. Briefing. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

7. European Union Agency for Railways (n.d.). Common Safety Methods. Available at: https://www.era.europa.eu/activities/common-safety-methods_en

8. Home Office (2022) all for information: Unauthorised access to online accounts and personal data. Consultation. Available online: https://www.gov.uk/government/consultations/unauthorised-access-to-online-accounts-and-personal-data/call-for-information-unauthorised-access-to-online-accounts-and-personal-data

9. Hoolohan, C., Amankwaa, G., Browne, A. L., Clear, A., Holstead, K., Machen, R., Michalec, O. & Ward, S. (2021). Resocializing digital water transformations: Outlining social science perspectives on the digital water journey. *Wiley Interdisciplinary Reviews: Water*, *8*(3), https://doi.org/10.1002/wat2.1512

10. Michalec, O. A., Van Der Linden, D., Milyaeva, S., & Rashid, A. (2020). Industry Responses to the European Directive on Security of Network and Information Systems (NIS): Understanding policy implementation practices across critical infrastructures. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (pp. 301-317). https://www.usenix.org/system/files/soups2020-michalec.pdf

11. Michalec, O., Milyaeva, S., & Rashid, A. (2021). Reconfiguring governance: How cyber security regulations are reconfiguring water governance. *Regulation & Governance*. https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12423

12. Michalec, O., Milyaeva, S., & Rashid, A. (2022). When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures?. Big Data & Society, 9(1), https://journals.sagepub.com/doi/full/10.1177/20539517221108369

13. Michels, J. D., & Walden, I. (2018). How Safe is Safe Enough? Improving Cybersecurity in Europe's Critical Infrastructure Under the NIS Directive. *Improving Cybersecurity in Europe's Critical Infrastructure Under the NIS Directive (December 7, 2018). Queen Mary School of Law Legal Studies Research Paper*, (291). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3297470

14. National Cyber Security Centre (2022). The Cyber Assessment Framework 3.1. Available at: https://www.ncsc.gov.uk/blog-post/the-cyber-assessment-framework-3-1

15. Topping, C., Dwyer, A., Michalec, O., Craggs, B., & Rashid, A. (2021). Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. *Computers & Security*, https://www.sciencedirect.com/science/article/pii/S0167404821001486

16. Wallis, T., & Johnson, C. (2020). Implementing the NIS Directive, driving cybersecurity improvements for Essential Services. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-10). IEEE. https://eprints.gla.ac.uk/223565/

Image credits

- Cover image: A Person inside a ship control room, by Sergii https://www.pexels.com/photo/a-person-inside-a-ship-control-room-14606488/
- Page 3: Plastic connectors in electronic switch on server, by Brett Sayles https://www.pexels.com/photo/plastic-connectors-in-electronic-switch-on-server-4657256/
- Page 10: Machines inside and Abandoned Factory, Muhammet Colak https://www.pexels.com/photo/machines-inside-an-abandoned-factory-7360328/
- Page 12: Close-up Photo of Control Panel, Ibrahim Boran https://www.pexels.com/photo/close-up-photo-of-control-panel-3582392/
- Page 16: The Chimney of Asco Nuclear Power Plant, Jorge Cubells, https://www.pexels.com/photo/the-chimney-of-asco-nuclear-power-plant-6742721/