Written evidence submitted by the Bristol Cyber Security Group (CYB0035)

The types and sources of cyber threats to Critical National Infrastructure (CNI) most critical to the function of the UK digital economy:

The types and sources of cyber threats to CNI may include state actors, cybercriminals, and insider threats. It is important to underscore the foundation for intelligence sharing and analysis of trends in cyber security to anticipate and mitigate these threats. It is important to consider the unique threat actors and attack types relevant to each sector:

- Communications (including space): threats include denial of service, distributed denial of service, sabotage, aimed to disrupt telecommunication and satellite networks.
- Energy: Attacks on power grid control systems, can be by state actors, ecological hacktivists, and cybercriminals.
- Government: espionage, potentially by state-sponsored groups, have a potential to undermine integrity and confidentiality.
- Finance: cybercriminals often target financial systems for monetary gain through ransomware or data breaches.

There is a continuous threat of ransomware that can cause large disruption to CNI, with recent examples such as the 2015 Ukrainian power grid attack, 2017 WannaCry attack which affected many aspects of CNI, in particular the National Health Service, and the 2021 Colonial Pipeline attack which resulted in fuel shortages across the Eastern US. While it is challenging to estimate the impacts of CNI attacks, academic and industry reports estimate the attack on the Ukrainian power grid in 2015 disrupted the power supply for thousands[1]. Within the ongoing Russia-Ukraine conflict, the Russian-linked Sandworm group has again successfully targeted the Ukrainian power grid as recently as 2022, as discovered by Mandiant[2]. Meanwhile, IBM reports that the average cost of a data breach in the energy industry is 4.65 million dollars[3].

There are an increasing number of sophisticated malware toolkits with a focus on disrupting CNI, such as the INDUSTROYER malware used in the Ukrainian power grid attacks in 2016[4] and the more recently discovered INCONTROLLER/PIPEDREAM malware discovered in 2022[5],[6] which can directly interfere with industrial processes. The use of such toolkits, if targeted towards UK CNI, poses a serious threat.

Cyber security attacks across the CNI sectors are worth particular consideration due to the prevalence of legacy systems that operate critical processes. Legacy and non-legacy systems

---

[1] Michael J Assante. 2016. Confirmation of a coordinated attack on the Ukrainian power grid. SANS Industrial Control Systems Security Blog 207 (2016).

[2] https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

[3] IBM. 2021. Cost of Data Breach. https://www.ibm.com/account/reg/us-en/signup?formid=urx-50915

[4] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

[5] https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/

[6] https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool

operate in tandem. Consequently, they are not always secured with the state-of-the-art technologies and practices due to lack of compatibility or CNI security skills gap[7]. Supply chain security is another key threat, especially the complex and intricate supply chains for CNI and varying standards and guidance across sectors in this regard.[8]

Finally, it's important to consider that not all cyber security attacks which affected critical infrastructures were originally targeting them. The case of WannaCry affecting the NHS was effectively an example of collateral damage[9]. WannaCry was a type of ransomware targeting Microsoft computers through encryption of data in exchange for a payment. The attackers did not plan on disrupting ambulances or medical devices as such. The WannaCry attack demonstrates the importance of looking beyond 'the usual suspects' when it comes to threat assessments.

The strengths and weaknesses of the UK Government's National Cyber Strategy 2022 and Government Cyber Security Strategy 2022-2030 in relation to CNI for the digital economy:

The strategies' strengths lies in their comprehensive approach, aligned with global cyber security policies. Additional strengths include the following:

- The strong emphasis on international and national collaboration;
- The proactive approach to building cyber skills within the workforce;
- The inclusion of 'secure by design' principles as a key component of the strategic initiative;
- The real-time threat analysis service for cyber security incidents at a national level;
- The foundation for the public awareness campaigns.

However, the strategies could be made more flexible through adding more dynamic and adaptive policy frameworks, that can incorporate new threat intelligence without changing the overall strategy. This agility is crucial for CNI, facing an increasing pace of technological development. In practice it would involve a combination of regular updates, modular approaches, rapid response capabilities, and feedback mechanisms.

Whilst the National Cyber Strategy broadly addresses the cyber security skills gap, it lacks specific focus on the underlying issue that affects the security of CNI, in particular the education of the workforce with relevant experience and knowledge of Operational Technology (OT) security[10]. OT has a direct impact on CNI, in particular acting as the key digital technology driving the water, energy, manufacturing and transport sectors – an area with little coverage within UK cyber security education. Across the large number of NCSC-certified[11] cyber security degrees, only one provides a focus on infrastructures security.

---

[7] https://www.usenix.org/system/files/soups2020-michalec.pdf

[8] https://uob-my.sharepoint.com/:w:/g/personal/le3977_bristol_ac_uk/EROaMkqZzE9Nk_PMikXacMkBFwcM1JNQ86grA85T1gR9jQ?email=awais.rashid%40bristol.ac.uk&e=XLTO3h

[9] https://www.economist.com/leaders/2017/05/20/the-wannacry-attack-reveals-the-risks-of-a-computerised-world

[10] https://industrialcyber.co/news/ot-security-skills-gap-is-a-major-challenge-for-industrial-manufacturing-organizations/

Sector-specific cyber security maturity models should be introduced that provide a roadmap for CNI agencies and organisations to assess their current capabilities and plan further improvements. This could be benchmarked against the global cyber security standards and strategies, to ensure global best practices are integrated into the UK's approach, implementing national campaigns to raise awareness about the importance of cyber security in CNI sectors, fostering the cyber security culture. Vice versa, the UK should be taking the lead and setting international standards and best practices both in terms of technology and development of workforce capabilities.

These strategies set the stage for improving sector-specific cyber security guidelines, to address unique challenges in specific CNI sectors, further fortifying the digital economy and national security, and contribute to the broader resilience of the UK's society and infrastructure, ensuring the continuity of critical services.

The effectiveness of the strategic lead provided by the National Security Council, Government Departments and agencies, and the National Cyber Security Centre, and the coherence of cross-government activity;

Based on our study concerned with the water sector implementation of NIS Regulations[12], we found that the relationships between the government bodies (e.g., Ofwat and Drinking Water Inspectorate) were not developed to a sufficient degree, leading to unfortunate strategic mismatches. For example, CAF inspection timescales were not aligned with 5-year funding cycles for water companies, effectively preventing them from investing in cyber security improvements in time. Additionally, we found that practitioners across sectors were discussing similar ideas (e.g., in the rail, energy and water industry, regulators and practitioners advocated for harmonising safety and cyber security guidance), but due to a lack of cross-government forum, they haven't developed a unified agenda[13].

It is essential to strengthen the National Cyber Security Centre's (NCSC) role in coordinating across government entities to prevent siloed efforts, ensuring that strategies are uniformly applied and effectively communicated. This can be accomplished through streamlining collaboration and communication protocols between government entities, CNI organisations, and academic experts, as well as ensuring that cyber resilience policies are implemented at all levels of government and critical sectors, with a particular focus on inter-agency cooperation. The NCSC already goes some way to facilitating this cooperation with the Industrial Control Systems Community of Interest (ICS-COI)[14], which currently consists of over 350 members across government, industry and academia. As well as providing information sharing amongst members, the COI operates various expert groups on specific topics, such as supply chains and vulnerability management, which produce guidance for the wider community including CNI operators.

---

[11] https://www.ncsc.gov.uk/information/ncsc-certified-degrees

[12] https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12423
https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12423 (Reconfiguring governance: How cyber security regulations are reconfiguring water governance; Michalec, Milyaeva, Rashid)

[13] https://ritics.org/wp-content/uploads/2023/06/Whats-next-for-NIS-RITICS-report-final-310123.pdf (What's next for the NIS Regulations?, Michalec)

[14] https://ritics.org/ics-coi/

This would also facilitate of a more dynamic response mechanism that allows a rapid adaptation to added information and events, backed by an adaptive legislative and executive support.

Based on our research on information sharing practices in UK CNIs, we recommend that the UK urgently needs to develop a coherent stance on information sharing across the CNI sectors (both nationally and internationally)[15]. Currently, operators are required to report critical incidents under NIS Regulations, but this does not include 'non-critical incidents' 'near misses' or information on the evolving threat landscape (e.g., potential attackers). The dilemma lies in the fluid nature of the above terms. On the one hand, encouraging reporting of the ongoing threats improves the collective intelligence of the CNI sectors. On the other, if a threat reported by one organisation turns into an incident in another, both organisations may be receiving fines. As a result, these contingencies of threat reporting pose a risk that operators will minimise their reporting altogether. The evidence from the critical infrastructure security regulations in the United States shows that fear of fines created a counterproductive environment for information sharing[16].

The effectiveness of the Government's relationships with, respectively, private-sector operators and regulators in protecting and preparing CNI organisations of most critical to the UK digital economy from cyber-attacks;

Our research found that the informal or voluntary public-private sector initiatives were particularly successful in improving the cyber security capability in UK CNI[17]. Based on a case study of NIS Regulations implementation across the water and energy sectors, we found that the most successful collaboration sharing initiatives were informal groups working towards a creation of a new industry standard or advising the Drinking Water Inspectorate on the scope of CAF. Originally CAF was written with IT systems in mind, ignoring the threats and vulnerabilities typical to OT systems found in industrial settings. Another success story is a voluntary sector-wide gap assessment conducted by a semi-formal working group in the energy sector, which enabled stakeholders to appreciate the differences in maturity between the most and least secure operators[18].

We offer the following recommendations:

- Establish clear channels for rapid information exchange and joint cyber incident response exercises. It is imperative to establish robust communication frameworks that facilitate real-time information exchange among CNI stakeholders. This entails not only the technological capability for rapid data transfer but also the procedural and legal frameworks that enable it.

---

[15] https://journals.sagepub.com/doi/full/10.1177/20539517221108369 (When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures?, Michalec, Milyaeva and Rashid)

[16] Clark-Ginsberg A, Slayton R (2019) Regulating risks within complex sociotechnical systems: evidence from critical infrastructure cybersecurity standards. https://doi.org/10.1093/scipol/scy061

[17] https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12423 (Reconfiguring governance: How cyber security regulations are reconfiguring water governance, by Michalec, Milyaeva and Rashid))

[18] https://ritics.org/wp-content/uploads/2023/06/Whats-next-for-NIS-RITICS-report-final-310123.pdf (What's next for the NIS Regulations?, Michalec)

- Regular cyber incident response exercises, as mentioned in the National Cyber Strategy 2022, should be conducted collaboratively across public and private sectors to simulate threat scenarios, refine response protocols, and reinforce trust through transparency and partnership. Such exercises will not only test and improve incident handling but also foster a culture of continuous learning and mutual support, which is crucial for maintaining the resilience of the UK's digital economy.
- Develop systematic programmes to upskill the UK's Cyber Workforce with regards to the specific systems and technologies underpinning CNI. Our experience shows that IT security expertise does not readily translate to OT security. There is an urgent need to develop workforce capability to ensure security and resilience of UK CNI.

What are the interventions that are required from Government, and CNI organisations most critical to the UK digital economy to ensure the Government's cyber resilience targets by 2025 are achieved;

Prioritise the implementation of the NCSCs Cyber Assessment Framework (CAF) across CNI sectors and ensure that cyber security is integrated into organisational governance. The following aspects should be considered:

- Quantitative analysis – statistics on past cyber incidents impacting CNI and their economic impact, that is essential for the contextualisation of resilience measures;
- Investment in Cyber security Skills – initiatives for investment in education, training and professional development, to aim to close the cyber security skills gap;
- Technology adoption – further evaluation of the integration of emerging technologies could strengthen cyber resilience;
- Legislative support – legislative measures that can enforce cyber security standards and penalties for non-compliance, alongside the method to evaluate non-compliance;
- Supply chain security – facilitate further discussions on the importance of securing the supply chain for CNI and how this can be achieved through stakeholder collaboration and 'secure by design' practices.

In the workshops with NIS Regulators and Operators, we noticed that the most common criticism regarding the CAF was its potential to become a 'tick box exercise'. Executives were often focused on achieving the best scores, rather than improving their security posture. We recommend the following practices to improve the implementation of the CAF[19]:

- Competent Authorities 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 be under pressure to achieve 'green' Indicators of Good Practice at all costs.
- Competent Authorities 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'.

[19] https://ritics.org/wp-content/uploads/2023/06/Whats-next-for-NIS-RITICS-report-final-310123.pdf (What's next for the NIS Regulations?, Michalec, RITICS Fellowship Report)

- Competent Authorities highlight the need to undertake continuous maintenance of the 'green' CAF status. Operators ought to include CAF cyber security measures as their business-as-usual and prepare a long-term programme 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.

What role will 'secure by design' and emerging technologies play in the cyber resilience of CNI most critical to the UK digital economy and their supply chains.

The effective incorporation of 'secure by design' principles alongside the adoption of cutting-edge technologies is pivotal for the cyber resilience of CNI. This is crucial not only for the protection of the UK's digital economy but also for the robustness of its supply chains. Institutionalising 'secure by design' within the procurement policies ensures that security considerations are embedded from the onset of technological development, creating a secure foundational infrastructure.

The integration of sophisticated technologies, such as Artificial Intelligence (AI), the Internet of Things (IoT), and next-generation networking, into CNI introduces complex risks. It is imperative to interweave 'secure by design' tenets in the early development and procurement phases, thereby shifting from reactive risk assessment to proactive risk prevention. This change is fundamental in cultivating a CNI ecosystem resilient to current and future cyber threats.

However, 'secure by design' is not a panacea. A holistic security framework is critical for the cyber resilience of CNI to provide robust protection that spans all aspects of infrastructure. Such a framework is built on the following pillars:

- **Hardware Security:** The DSBD.tech initiative and CHERI/CHERIoT architectures have significantly advanced hardware security. Yet, this is merely the foundation upon which additional security layers must be built.
- **Software Integrity:** As the Heartbleed bug incident revealed, a critical oversight in software, such as a flaw in the OpenSSL cryptography library, can have widespread repercussions. Effective security demands secure coding practices and regular vulnerability assessments to complement hardware defences.
- **Network Defences:** The SolarWinds breach exemplifies the nuances of network security, highlighting the necessity for secure update mechanisms and transmission protocols to protect against sophisticated cyber-attacks.
- **Data Protection:** GDPR mandates underscore the need for rigorous data protection strategies, including encryption and access control measures to prevent unauthorised data breaches.
- **Human Factors:** The resilience of technical measures can be undermined by human error. A comprehensive approach to cyber security recognizes the importance of security awareness and training in software developers, security engineers and architects as well as end users to ensure that *secure by design is a philosophy across the socio-technical system* and not merely a technological consideration.

These elements are not standalone; they are interconnected. For example, secure communication protocols and encryption are as crucial as the secure hardware they run on, and the human factors element necessitates a security-aware culture to enhance technical safeguards. *In* our recent research, we interviewed energy cyber security practitioners about their experiences with the 'security by design' paradigm.[20] We concluded that, in this case standardisation bodies (e.g., British Standards Institute) ought to collaborate with social scientists and third sector organisations to resolve the tension between the need to create a benchmarked security standard in the industry and the requirement to make smart technologies tailored to underserved populations. Inclusion ought to reach beyond the Equalities Act (2010) assessment, i.e., provide tailored security support for people without multiple devices (relevant to multi factor authentication), without digital skills (relevant for configuration or updates) or those using older generation devices which aren't interoperable with smart appliances.

In the realm of 'secure by design', a comprehensive security framework is imperative, one that synergises secure hardware capabilities, such as those enabled by the CHERI architecture, with rigorous software security protocols. CHERI's fine-grained memory control not only mitigates vulnerabilities but also facilitates the compartmentalisation of memory access. This compartmentalisation inherently aligns with GDPR's data protection mandates by constraining the extent of data exposure and reducing the impact of potential breaches. When harmonised with secure coding practices and strict adherence to established security protocols, this approach embeds security and privacy at the core of the system and localises risks. In parallel, robust network defences are crucial, demanding the implementation of secure communication protocols and thorough monitoring to pre-empt cyber threats. This multi-layered defence strategy ensures that each element of the CNI's security framework contributes to a collective resilience, providing a comprehensive defence against cyber threats while strictly adhering to data privacy standards.

In conclusion, the 'secure by design' *philosophy* is foundational to an effective security framework for CNI, anchoring an ecosystem that includes secure hardware, robust software development, stringent encryption, and meticulous data management, all upheld by a culture of security awareness. This strategy endorses compartmentalisation at the procedural and data levels, which serves as a safeguard against systemic failures and confines the impact of any breaches, thus maintaining the operational integrity of the network. To implement and sustain this framework, a skilled workforce is indispensable; professionals adept in these technologies are the linchpin in evolving CNI defences. With their expertise, coupled with stringent regulatory standards and a proactive approach to adapting to new threats, the UK can solidify its CNI against diverse cyber risks, ensuring the security and resilience of its digital economy and its essential supply chains.

We reaffirm the commitment to UK cyber security resilience.

The emphasis on cyber innovation positions the UK to lead in the development of the cutting-edge cyber defence technologies.

---

[20] https://doi.org/10.1016/j.erss.2023.103327 (Who will keep the lights on? Expertise and inclusion in cyber security visions of future energy systems; Michalec, Shreeve and Rashid)

10 November 2023