Written response to the House of Commons DSIT Committee Inquiry “Cyber Resilience of the UK’s Critical National Infrastructure”

PETRAS National Centre of Excellence for IoT Systems Cybersecurity

November 2023

Contributors

Dr. Gideon Ogunniye
Amaya Hana
Dr. Nilufer Tuptuk

Introduction

The PETRAS National Centre of Excellence for IoT Systems Cybersecurity exists to ensure that technological advances in the Internet of Things (IoT) are developed and applied in consumer and business contexts, safely and securely. This is done by considering social and technical issues related to the cybersecurity of IoT devices, systems, and networks. The Centre is a collaborative, multidisciplinary effort bringing together academics from 24 UK Universities, 120+ Industrial and NPO partners, and 63 research projects, led by the University College London in collaboration with Imperial College London, University of Warwick, University of Oxford, and Lancaster University. We have previously responded to the DSIT’s 'Establishing a pro-innovation approach to regulating AI' consultation[1] and the Tech Horizons Report 2022 of ICO[2] and are pleased to provide evidence for this inquiry. Using examples taken from PETRAS projects and the findings and recommendations from PETRAS industry-specific workshops, covering several UK CNI sectors including energy, health and finance, among others, this evidence highlights the importance of **establishing a cross-sectoral regulatory framework for knowledge sharing and communication between the Critical National Infrastructure (CNI) sectors, to share incident reports, mitigations and engineering fixes, among others, that can make all sectors safer.**

Key Points

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

The UK’s CNI is critically dependent on digital technologies that provide communications, monitoring, control, and decision-support functionalities. Digital technologies are progressively enhancing the efficiency, reliability and availability of infrastructure, and enabling new benefits not previously available. However, as technology becomes more advanced, so are cyber criminals. One of the most critical cyber threats to CNI would be the use of Artificial Intelligence (AI) to develop new methods of attack that can be difficult to

[1] https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement
[2] https://ico.org.uk/about-the-ico/research-and-reports/tech-horizons-report/

protect against and the consequences of this can be catastrophic. Using AI and the Internet of Things (IoT) in CNI systems opens up new vulnerabilities and entry points to larger systems[3].

Threat actors may exploit AI for their gain in the following ways:

- Develop autonomous attacks by identifying vulnerabilities and attack surfaces in CNI systems and exploiting them.
- Create reconnaissance attacks and intelligence gathering.
- Analyse existing system defences and develop attacks against those defences or adapt to existing security controls. For example, an AI-driven Distributed Denial of Service (DDoS) attacks or malware that evades detection systems.
- Deep fake technology can be exploited to spread misinformation; develop advanced social engineering attacks (phishing attacks); and manipulate or create fake evidence for criminal cases.

However, AI can also enhance the detection of attacks and intrusions by leveraging its ability to analyse vast amounts of event and communication data, identify patterns, and recognise anomalies.

Some CNI sectors and their most probable threat actors.

- **Communications (including space)**
  - Disruption of communication networks through DDoS attacks (terrorist groups, state-sponsored and nation-state actors, etc.). CNI such as the rail and water network are heavily dependent on communication.
  - Hybrid (cyber-physical) attacks on infrastructure (terrorist groups, state-sponsored and nation-state actors etc.).
  - Supply chain attacks – using compromised hardware and software (terrorist groups, state-sponsored and nation-state actors etc.).

- **Energy**
  - Ransomware attacks (career cybercriminals). The push towards net zero with high penetration of renewable energy can further exacerbate the vulnerability of the power grid to cyber-attacks. IoT-based smart energy devices pose new attack vectors for the power grid. Most threats to the UK energy sectors come from the consumption side, as home devices (EV chargers, smart hubs, etc.) are created by third parties and used by consumers with little or no security practices. PETRAS Project PrivIoT explores digital harms in the interaction between home IoT devices, smart meters, and Demand-Side Management (DSM) technologies, and develops conceptual tools to improve users' situational awareness and agency[4].
  - Attacks against cyber-physical systems (terrorist groups, nation-states, state-sponsored actors, etc.).

[3] Epiphaniou, G., Hammoudeh, M., Yuan, H., Maple, C. and Ani, U., 2023. Digital twins in cyber effects modelling of IoT/CPS points of low resilience. Simulation Modelling Practice and Theory, 125, p.102744.

[4] https://petras-iot.org/project/understanding-and-mitigating-privacy-risks-of-iot-homes-with-demand-side-management-priviot/

  - Disinformation campaigns (hacktivists and competing energy companies, etc.).

- **Government**
  - Espionage and data breaches (insiders, contractors, nation-states and state-sponsored actors).
  - Disinformation campaigns (hacktivists, nation-states and state-sponsored actors).

- **Finance**
  - Ransomware (career cyber criminals).
  - Phishing attacks (cyber criminals).
  - Cyber-attacks disrupt market manipulation (career cyber criminals).

2. 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

Strengths

The five pillars of the National Cyber Strategy 2022 emphasise the importance of a multistakeholder approach involving shared responsibilities between government authorities, industry and academia towards cybersecurity capacity building and knowledge sharing and communication. **Cybersecurity is a shared responsibility that requires coordinated actions from the stakeholders involved.** Findings from PETRAS industry workshops show clear unanimity across CNI sectors (energy, finance, health, and transport, for example) on the importance of **establishing a cross-sectoral regulatory framework for knowledge sharing and communication**[5]. As geopolitical tensions have led to attacks targeting CNI, stakeholders in the sectors should be encouraged to share among themselves and with research institutions, incident reports, mitigations and engineering fixes, among others, that can make all sectors safer.

The strengths of the National Cyber Strategy 2022 and the Government Cyber Security Strategy 2022 - 2030 include.

- Development of skills and knowledge of the existing workforce.
- Support for innovation, research, and development.
- Focus on cyber resilience.
- Partnership with international partners to tackle cyber threats and achieve resilience.

Weaknesses

While we agree that the National Cyber Strategy 2022 and the Government Cyber Strategy 2022 -2030 lie at the core of efforts to insulate the public sectors of the UK from cyber threats, we, however, suggest that **the strategy must be complemented with domain-specific guidelines to address cyber threats in various sectors and industries of the**

[5] PETRAS will host an online briefing on 18 December 2023 to discuss the findings and recommendations from the workshops. See https://petras-iot.org/update/future-challenges-of-iot-cybersecurity-in-uk-industry-sectors/

CNI. Findings from PETRAS industry workshops reveal that, while existing regulations/policies provide (reasonable) cybersecurity guarantees, **they are hard to implement**. This is because the threat actors across various sectors and industries are different, and, as such, policies/regulations don't often align with threats. Therefore, it is suggested that the **UK should seek to lead the development of prescriptive IoT cybersecurity policies and regulations for the CNI sectors**. Such policies and regulations should, for example, provide the definitions of safety, resilience, privacy, and security requirements for devices.

The weaknesses of the National Cyber Strategy 2022 and the Government Cyber Security Strategy 2022 - 2030 include.

- Implementation challenges: the absence of clear and quantifiable performance metrics.
- The threats associated with emerging technologies will be difficult to deal with.
  - The integration of new information and communication technologies (ICTs), such as sensors, data analytics, IoT, AI, and cloud computers into CNI systems that society depends on for services such as health, energy, transport, and agriculture, has created new risks, which may threaten the security of society, environment, and human well-being.
  - More efforts are required to develop domain-specific guidelines for the implementation of both strategies to deal with emerging and future threats.

3. The effectiveness of the strategic lead provided by the National Security Council (NSC), Government Departments and agencies, and the National Cyber Security Centre, and the coherence of cross-government activity.

The strategic lead provided by the National Security Council and other relevant government departments will be effective in developing a cross-sectoral regulatory framework for knowledge sharing and communications between CNI sectors on the forthcoming impacts of emerging technologies.

To achieve cyber resilience of the UK's CNI, the NSC (in collaboration with relevant government departments) should coordinate actions to ensure:

- Relevant public institutions provide public awareness of cybersecurity and safety.
- The creation of a common language for cyber security across CNI sectors by driving consensus among stakeholders. There is a need to align the standards of multiple industries and feed them into the high level of standards.

4. 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.

The private sector is often at the forefront of cyber security skills requirements because they are responsible for a large share of online activity and should play a larger role in ensuring cybersecurity. "In the context of a national cyber security skill shortage, the government struggles to compete with the private sector to attract and retain the required cadre of diverse and skilled cyber security professionals, despite its positive efforts to date'" (Government Cyber Security Strategy 2022 - 2030, Chapter 1, page 15). **The relationship between Government and private-sector operators and regulators is crucial to the co-creation of regulatory and knowledge exchange networks.**

In addition, **academia plays an important role in generating evidence for policymaking**. This role involves the analysis of the decision-making process of innovation policies. To develop policies, governments must have a knowledge of technological trajectories, market potential, and the capabilities and limitations of industrial actors, among others. Policies and strategies that manage risks must include an understanding of operator and corporate behaviour, as well as technical elements and the interfaces between them and humans[6]. Academia-government interactions will help develop policy tools to generate evidence, and these processes can be gradual and incremental, helping policymakers overcome the high level of uncertainty in emerging technology development.

5. 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?

Gaps exist in organisational understanding at several levels within the least aware CNI organisations[7]. At the most basic level, operators may not understand the degrees of vulnerability of the systems or the types and subtlety of attacks. More aware infrastructure organisations tend to deal with cybersecurity at a purely technical level and sparsely consider and include behavioural and other social factors. In addition, there is a big gap between government policies and industrial implementation.

The government should:

- Develop and enforce appropriate cybersecurity regulations and standards for the CNI sectors.
- Provide adequate funding for research and development. A national centre such as the PETRAS National Centre of Excellence for IoT Systems Cybersecurity should be established and properly resourced to carry out the following functions.
  - Provide a platform for knowledge exchange among stakeholders on initiatives in CNI systems.
  - Identify regulatory gaps and collaborate with regulators to address them, especially in the areas of emerging technologies.
- Develop effective incident response and recovery plans with measurable performance metrics.

6. 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?

Secure by design approach is crucial to ensure that software products and capabilities within CNI systems are designed in a foundational way to be secure, as it is an effective approach to minimise the impact of human factors on cybersecurity. Users and abusers

[6] https://petras-iot.org/wp-content/uploads/2022/02/MASS-policy-briefing-short.pdf
[7] https://petras-iot.org/wp-content/uploads/2022/02/Policy-Briefing-on-MS-for-CNI_v12-final.pdf

must be included in the design and analysis of cybersecurity. This would be a cost-effective solution to reduce vulnerabilities than building security into existing systems later.

Emerging technologies can strengthen the resilience of CNI.

- AI can be used for security monitoring, predictive analysis, and threat detection.
- IoT and 5G and beyond are essential technologies for data collection and management. For example, IoT can enhance environmental, social and governance (ESG) for the financial sector with better data.
- Blockchain technology can provide the traceability and integrity of transactions and data exchanges within CNI.