CYBER RESILIENCE OF THE UK'S CRITICAL NATIONAL INFRASTRUCTURE

10 November 2023

Assoc Prof Erisa Karafili
Dr Robert H. Thorburn
Prof Vladimiro Sassone

University of Southampton
Cyber Security Research Group
{e.karafili, robert.thorburn, vsassone}@soton.ac.uk

Contents

1 Executive Summary and Recommendations

UK critical national infrastructure is currently adapting IoT technology for increased efficiency and security. Since these technologies include remote sensing, data processing, and networking, a number of key cyber security and resilience-related questions must be asked. These include citizen's perception of the usage of such technology in critical infrastructure, the hardware involved, and the manner in which attacks against these systems can be traced and attributed. In this report, we discuss the first point by way of a study examining public trust in such systems, the second by examining both current hardware and new developments with a specific focus on the UK, and finally, we turn to the question of attack attribution in critical infrastructure. These discussions are then also framed in reference to the five pillars of the UK's national Cyber Strategy.

We recommend that the government should:

- Provide clear non-technical device, service, and system details to citizens.
- Provide clear explanations on data gathering, data storage, and security measures.
- Should continue its exemplary work in advocating for, engaging with, and funding UK research and development for security by design and related systems and hardware such as the CHERI architecture.
- Should direct procurement to UK hardware wherever feasible.
- Should promote, and invest in further research on, technologies that tackle the issue of attack attribution such as formal reasoning and neuro-symbolic AI.

Response authors

Dr Erisa Karafili is an Associate Professor in Cyber Security at the University of Southampton. Previously, she was a Marie Curie Fellow at the Department of Computing, Imperial College London. Her main research areas are cyber-attack attribution, formal methods applied to security and privacy problems, data Sharing in cloud environments, data access control, threat models for IoT and hybrid systems.

Dr Robert Thorburn is a research fellow in Cyber Security at the University of Southampton. Robert's research includes privacy, systems design, and the IoT. He currently works on the integration of Morello and off-the-shelf hardware, as well as related modelling and design.

Professor Vladimiro Sassone is RAEng Research Chair in Cyber Security at the University of Southampton. Vladimiro's research interests include data privacy, anonymisation, the IoT, provenance, blockchain, internet and cloud computing, social and human factors in cyber, cyber-crime, foundations of computation, machine learning, and AI.

2 Improving the citizens perception on the usage of IoT technology in Critical Infrastructure

2.1 Motivation

We are seeing an unstoppable need for the modernisation of the national critical infrastructure in order to make it more efficient and also to increase its security and safety. Technologies like IoT systems are being used and adapted in various sectors of our national infrastructure. To ensure a smooth implementation of such technology, we need to take further factors into consideration, e.g., risk, threats, adaptability. An important factor that has not been carefully considered is the **user** factor. How the users interact with these devices, their knowledge, and their perception is very important as it plays a crucial role in the successful implementation of such technologies, as well as in preventing attacks where humans play a role in them.

2.2 Background

User's perspectives on how IoT devices work can have a significant impact on their acceptability [5] of such technologies. There have been studies on the different factors affecting user's acceptability [11][10] and resistance [19] of a system, in particular, user-centric frameworks and paradigms for IoT technology [1]. Research has been conducted into user perceptions on IoT-based healthcare [5], smart home security [27] and smart home personal assistants [2][3]. Currently, there is a limited amount of work on users' perception of the implementation and acceptability of IoT devices [8]. Most importantly, there have been no work on the usage and security of IoT devices within the critical infrastructure.

In order to fill the gap in this important and critical sector and to provide further recommendations to the IoT technology manufacturers and adaptors in the critical infrastructure, we performed a study on the users' perception on the usage of IoT technology in the national critical infrastructure.

2.3 Our Study

In 2022 we conducted a qualitative study [4] to analyse the *citizen perception* on the usage of IoT devices in the Critical Infrastructure. The study was in the form of a questionnaire that was answered by 125 participants from the UK. Overall, from this study, we concluded that the users' acceptance of the usage of IoT devices in the critical infrastructure depends on the perceived benefits, their level of understanding of the device as well as their confidence in using and maintaining the device.

Our study asked the users to answer questions about their level of understanding of the technology and its benefits, the likelihood of consent to the usage of this technology, consent to data collection from the devices, as well as their perception of the security of these devices. In the study, we provided specific case studies for the following critical infrastructure sectors: *finance*, *emergency services*, *energy*, and *health*, where different cases of IoT technology usage were provided to the participants.

2.4 Main Findings

Our study showed that the likelihood of the participants using the proposed devices in the various critical infrastructure scenarios was average (between neither unlikely nor likely and somewhat likely). The results suggest that there is not a complete rejection of this technology. Thus, further work needs to be done in order to improve the users' acceptability.

Our analysis of the results provided some further useful insight. It showed that perceived benefit, level of understanding, confidence in learning to use, self-trust to use and maintain, and in some instances, device usability influence how likely a user is to use a device. We believe that this information is useful to improve the acceptability of such technology and increase the level of trust the citizens have in the adaptation of this technology into the national critical infrastructure.

Another finding dealt with the participant's perception of the level of security of the IoT technology, as the majority answered neither insure nor secure. Thus implying that the users require more information about the security aspect of the implemented IoT devices.

2.5 Recommendations

Our main recommendation is in order to increase the users' acceptability of such technology in the critical infrastructure sector, thus increasing the level of trust, the *citizens need to have more information about the technology.*

The manufacturers as well as the adaptors of the IoT technology into the critical infrastructure need to be transparent with the users about the security levels of the implemented technology to increase the citizens' level of trust. Furthermore, there is a need for more marketing and awareness campaigns in order to increase the level of knowledge of the citizens on such devices, thus, increasing the level of acceptability of this technology.

Below is provided a more detailed list of recommendations:

- Provide users with clear information, in plain language, on how the devices are kept secure from threats.
- Provide a clear non-technical explanation of the device and its purpose to improve users' understanding.
- Aim to inspire confidence in users to learn to use the technology and improve their levels of self-trust to use and maintain the device, for example, with tutorial videos or workshops.
- Provide more information about the data usage and customized options for sharing data.

3 Hardware and Design for Critical Infrastructure

3.1 The Hardware Landscape

The protection of critical infrastructure against cyber threats presents the government with a far-ranging policy challenge [26] due to not only the importance of the infrastructure concerned but also the continuing divergent development of networking, interfacing, and security technologies. The latter three points specifically relate to the manner in which distributed computing and sensing have become ubiquitous, as commonly lumped under the term IoT (Internet of Things) [20]. A full exploration of the IoT and its continuing development would be too expansive to include herein, so instead the focus here will be on current and upcoming technologies which are not only of key importance, but also have a specific significance to UK research, development, and industry.

The first of these is ARM Holdings PLC. Headquartered in Cambridge, Arm and its similarly named ARM architecture is at the forefront of chip design and holds significant market share, especially in mobile and embedded devices but also a range of other applications including industrial control systems [28]. This broad-ranging application also implies that ARM-based security protections, such as ARM TrustZone [21], are widely used not just in the UK but internationally.

The next significant player is RISC-V, which is the current and most prominent iteration of the reduced instruction set computer (RISC) architecture. RISC-V is an open standard with an extensive and collaborative international effort behind its development. This development has made significant progress and a wide range of RISC-V implementations are available ranging from application-specific modules to single-board computers. One of the stand-out features that has accelerated this adoption is a modular design approach allowing users to include or exclude functionality based on their specific needs [13]. It is therefore also no surprise that the UK is involved in RISC-V research and development efforts including the extension and enhancement of RISC-V security by way of the CHERI architecture, which is discussed in Subsection 3.2.

The ease with which significant technologies can be pointed out though, belies the deeper challenges relating to embedded systems, larger systems of systems and especially, networked systems. Embedded systems and Internet of Things devices are heterogeneous by nature [24], in large part due to the lowered component costs coupled with ease of customisation. This intrinsic heterogeneity undermines efforts to harmonise and secure technologies across a network, with security further undermined by a range of memory safety and other weaknesses in some of the most widely used programming languages [22]. Unsurprisingly, these characteristics and related challenges also hold for critical national infrastructure [7]. It is accordingly no surprise that there has been a significant effort both in the UK and internationally to further the cause of taking a “secure by design” approach to the development of critical national infrastructure. However, taking a “by design” approach to addressing challenges in hardware design is applicable across the board for all requirements not only security, as was shown in our work treating regulatory compliance in hardware as a design issue. Specifically by developing a domain extension to SysML (Systems Modelling Language) to incorporate the requirements of the UK Data Protection Act [23]. In the following subsections, we first consider current research and development work in the UK and then consider opportunities for leveraging these resources within the context of the National Cyber Strategy.

3.2 Research and Development in the UK

Memory safety and other inherited weaknesses in languages such as C and C++ represent a significant security challenge in all implementations including the technology used in critical infrastructure. As such, it is a prime target for research. Over the past decade, this issue (and related challenges) has been the focus of a major UK-led research and development initiative called CHERI (Capability Hardware Enhanced RISC Instructions). The CHERI project is a joint venture by SRI International and the University of Cambridge which aims to update certain hardware design choices in aid of significantly improving system security. This project is not only notable for the extensive amount of work and progress demonstrated, but also for the broad-ranging support it has gained from multiple local and foreign parties including universities, private enterprises and governments, with significant contributors including DARPA, ARM, UKRI, Google and Microsoft. In terms of the UK's National Cyber Strategy [14], these strongly speak to the second and third pillars, namely technological advantage and global leadership. This advantage is also being extended further with multiple projects targeting the application of the CHERI architecture to current challenges, the most prominent of which is the Morello project.

Developed as an implementation of the CHERI architecture, the Morello project brings fine-grained memory protection to ARM processors. This is not only notable for the advancement in security and secure-by-design applications it brings, but also for both technologies being developed in the UK. The Morello project not only involves the boards developed and provided by ARM, but also the larger Digital Security by Design project managed by UKRI, which has distributed Morello boards to various private sector, government, and academic researchers, including the University of Southampton. The UK government interest mentioned here includes a range of potential security applications extending from traditional cyber security to military applications.

Morello is, however, not the only implementation of the CHERI architecture. One particularly rich stream of research and development is that relating to RISC-V processors. This implementation, known as CHERIoT (Capability Hardware Extension to RISC-V for Internet of Things), implements CHERI in RISC-V for use in embedded systems. The CHERIoT architecture was developed by Microsoft but two UK entities are involved in taking this through to implementation. These are LowRISC and SCI Semiconductor Ltd, both based in Cambridge. LowRISC will be publishing its open standard and making a number of boards available to researchers early in 2024. These CHERIoT boards will also be compatible with LowRISC's existing data centre offering which was developed in conjunction with Google.

3.3 Leveraging UK Expertise for Securing Critical Infrastructure

As discussed in the UK National Cyber Strategy 2022 [14], the three key aspects of cyber resilience are understanding the nature of the risks involved, attack prevention, and impact minimisation of successful attacks. Considering secure by design solutions such as the CHERI architecture, it is clear that these fit the bill, especially in terms of the first and second aspects of cyber resilience.

Formulating a "by design" solution to challenge and impact of hardware on cyber resilience within critical national infrastructure, might seem to be hindered by the prevalence of disparate requirements and heterogeneous technologies. However, it is exactly in taking a design-led approach that these challenges can be addressed and ultimately overcome. A clear example of this is the approach taken by the Ministry of Defence in adopting the NATO Architecture Framework which standardises architecture development and definition as part of a design-led approach. This is also not a new development as the MOD previously used the Ministry of Defence Architecture Framework (MODAF) which it developed. The main takeaway from this example is that taking a "by design" approach necessarily compels one to also consider how to track, conduct, and manage the design process.

Research on the management of the design process is also being conducted in the UK and specifically with relation to the implementation of CHERI-based systems. As part of the HD-Sec (Holistic Design of Secure Systems on Capability Hardware) project at the University of Southampton, work is being done on not only integrating CHERI-based hardware into systems containing heterogeneous off-the-shelf components but also on streamlining the design process when using systems modelling in combination with formal modelling for the design of secure systems [25].

In the preceding discussion, we introduced prominent technology with direct relevance to any networked system, but specifically also to critical national infrastructure. Following that we discussed the continuing work being done in and led by the UK, to further harden these technologies against attack and exploitation. For a country such as the UK which faces a disproportionate level of cyber attacks, such technologies and the continuing work on them is of paramount importance, as is support and leadership from government in advancing these efforts. Here, work on the CHERI architecture and related hardware is a great example since the direct guidance and financial support from HM government played a significant part in the results realised thus far. To conclude this section then, we consider the ways in which HM government can proceed to realise its 2025 priority actions, the five pillars [14], with reference to the issues of distributed compute and sensing hardware in critical infrastructure, secure by design, and related research.

Recommendations per pillar:

- **Pillar 1:** Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry
  - The UK's Digital Security by Design programme and the larger CHERI ecosystem has excelled at promoting and supporting local research and expertise. These initiatives should be built on with further funding and support by way of direct research funding such as that offered by UKRI, as well as by industry partnerships and collaboration.
  - The UK's Digital Security by Design programme also provides a blueprint for future initiatives, where interested parties from academia, industry, government, and across divergent disciplines, were drawn in from the outset. Key goals in this were networking and interdisciplinary collaboration.
  - Skills building does not, however, start at the point of developing secure hardware but rather at the point of education and training feeding into the research organisations concerned. On this count, STEM education across the piece from schools to universities, remains a key area in need of continuing support and funding.

- **Pillar 2:** Building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected
  - The UK's leading position with regard to the technology described herein is not only located in the development and research work but also in bringing those technologies to market. This brings a doubling of economic benefits, as there is not only the direct benefit from the associated economic activity (employment, manufacturing, etc) but there are also the reduced costs associated with more secure systems suffering fewer costly cyber attacks. Although the issue here is critical national infrastructure, the cost implications remain and as such, greater involvement with these technologies should be advocated for.
- Pillar 3: Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies
  - As discussed in this report, the UK has a clear leadership position in the research, development, and commercialisation of the technologies presented here. This is an excellent position to be in and must be leveraged to further advance the UK's position. This includes advocating for, and directly supporting, the continuing development of CHERI-based systems, the integration of this technology into existing hardware, and procurement of such locally produced technology.
  - With regard to industrial capability, the UK has a significant opportunity when it comes to commercialising the fruits of the preceding research and design efforts. As locally designed hardware enters production, any appropriate channels from networking to direct procurement should be used to support these endeavours.
- **Pillar 4:** Advancing UK global leadership and influence for a more secure, prosperous and open international order, working with government and industry partners and sharing the expertise that underpins UK cyber power
  - The hardware discussed herein is both cutting edge and likely to develop and improve further whilst the needs relating to securing critical national infrastructure are bound to evolve over time. Accordingly, it is of the utmost importance that government, industry and academia maintain an open and collaborative stance which would not only be to the benefit of all parties but also align with the national interest.
- **Pillar 5:** Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace, making more integrated, creative and routine use of the UK's full spectrum of levers
  - The technology described herein specifically closes down a set of long-standing weaknesses in computer architecture present in processors from the desktop to embedded sensors and data centres. As such, the disruption and deterrence of

attacks happen at the hardware level. This is a significant step and provides the designers of critical national infrastructure with a powerful new tool.

- The existence and functioning of this hardware, especially with regard to embedded devices, should be brought to the attention of the procurement and design functions of the government and/or contractors tasked with the design and maintenance of critical national infrastructure.

4 Need for automatic tools for Attack Attribution in the Critical Infrastructure

4.1 Motivation

The severity and frequency of the cyber-attacks we are currently facing are expected to continue, especially given the exponential increase in the usage of IoTs and Edge Computing. These attacks come along with the increased economic costs associated. When dealing with cyber-attacks in national critical infrastructure, the damages to the economy as well as to the citizens' trust in the nation's infrastructure are disastrous.

We are seeing that existing protective and mitigating measures are not sufficient to cope with the sophistication of current attacks. Thus, there is a need to enforce efficient **attacker-oriented countermeasures**, i.e., countermeasures that are specific to the attacker or group of attackers performing the attack. Identifying who performed an attack and bringing the perpetrators to justice (for example through sanctions when dealing with state attacks) can act as a deterrent for future cyber-attacks.

Attributing cyber-attacks, especially the ones that has as target the critical infrastructure of a nation, is extremely important but also a challenging problem, and it stands in between *Pillar 2: Cyber Resilience* and *Pillar 5: Countering Threats* of the National Cyber Strategy [12].

4.2 Current State of Attribution

Currently, the attribution process is mainly human-based, hence easily biased and error-prone, and labour intensive as it involves skilled human resources to analyze enormous amounts of low-format data [9].

- *Digital forensics* techniques help during the attribution process but they suffer from the limitations derived from the big amount of data to be collected and analyzed [6, 15].

- *AI- and ML-based tools* have been recently developed to help the detection and analysis process (e.g., through IDS and SOC tools) by providing information about the attack and possible next steps. The problem is that these techniques are insufficient, crucially in that they rely on past data/attacks. As such (1) they are ineffective in tackling new attacks and in identifying novel patterns. (2) They suffer from false positives/negatives. (3) They lack of transparency. (4) These tools require large datasets, which are unavailable or scarce in the cyber-attack attribution context, and almost non-existent for the critical infrastructure.

To deal with the above problems there have been attempts to develop tools that help during the decision-making of the analysts during the cyber-attack attribution process [16, 17, 18]. The current solutions still are not able to provide the full automation of cyber-attack attribution.

There has been some funding allocated to the attribution problem (Dstl through DASA and Innovative UK), but still, it has been very limited support.

4.3 Next Steps

Neuro-symbolic AI promises to solve some of the issues, but it is in its infant state and further foundational work needs to be done to construct symbolic models that represent such processes.

Two important aspects need to be taken into consideration that are difficult to include in the current solutions and technology:

1. the *human intuition* that needs to be included in such process, thus, possibly emulated in the automation process;

2. the always evolving social and political *context* where the attack takes place.

Further support and funding should be provided to solve this important problem. This will enable the UK to retain the leadership position in the research and development of innovative technology in cyber security (**Pillar 1**), as well as in advancing UK global leadership and influence for a more secure international order (**Pillar 3**).

Acknowledgements

Dr Erisa Karafili wants to acknowledge Caitlyn Alexander, for her work on the study on the human perceptions on IoT devices [4]. Part of the results of her project were used to provide recommendations in this report.

Dr Robert Thorburn wants to thank the EPSRC for supporting both his doctoral research and the current HD-Sec project at the University of Southampton.

References

[1] Wafa Abdelghani, Corinne Amel Zayani, Ikram Amous, Florence Sèdes, and Abdelghani Wafa. User-centric IoT: Challenges and Perspectives. *UBICOMM 2018: The Twelfth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, pages 27–34, 2019.

[2] Noura Abdi, Jose M Such, and Kopo M Ramokapane. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*, 2019.

[3] Noura Abdi, Xiao Zhan, Kopo M. Ramokapane, and Jose Such. Privacy Norms for Smart Home Personal Assistants. *Conference on Human Factors in Computing Systems - Proceedings*, 5 2021.

[4] Caitlyn Alexander. User perspectives on using IoT technology for critical infrastructures. *University of Southampton*, 2022.

[5] Mansour Naser Alraja, Murtaza Mohiuddin Junaid Farooque, and Basel Khashab. The Effect of Security, Privacy, Familiarity, and Trust on Users' Attitudes Toward the Use of the IoT-Based Healthcare: The Mediation Role of Risk Perception. *IEEE Access*, 7:111341–111354, 2019.

[6] Brian Carrier. Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of Digital Evidence*, 1(4):1–12, 2003.

[7] Gianfranco Cerullo, Valerio Formicola, Pietro Iamiglio, and Luigi Sgaglione. Critical infrastructure protection: having siem technology cope with network heterogeneity. *arXiv preprint arXiv:1404.7563*, 2014.

[8] Pierre Ciholas, Aidan Lennie, Parvin Sadigova, and Jose M. Such. The Security of Smart Buildings: a Systematic Literature Review. 1 2019.

[9] Luís Filipe da Cruz Nassif and Eduardo R. Hruschka. Document clustering for forensic analysis: An approach for improving computer inspection. *IEEE Transactions on Information Forensics and Security*, 8:46–54, 2013.

[10] Anastasios A. Economides. User Perceptions of Internet of Things (IoT) Systems. *Communications in Computer and Information Science*, 764:3–20, 2017.

[11] Rino Falcone and Alessandro Sapienza. On the Users' Acceptance of IoT Systems: A Theoretical Approach. *Information 2018, Vol. 9, Page 53*, 9(3):53, 3 2018.

[12] GOV.UK. National cyber strategy 2022. `https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022`, 2022.

[13] Samuel Greengard. Will risc-v revolutionize computing? *Communications of the ACM*, 63(5):30–32, 2020.

[14] HM-Government. National cyber strategy 2022 pioneering a cyber future with the whole of the uk, 2022.

[15] Erisa Karafili, Matteo Cristani, and Luca Viganò. A formal approach to analyzing cyber-forensics evidence. In *ESORICS 2018*, pages 281–301, 2018.

[16] Erisa Karafili, Antonis C Kakas, Nikolaos I Spanoudakis, and Emil C Lupu. Argumentation-based security for social good. In *AAAI Fall Symposium Series; 2017 AAAI Fall Symposium Series*, pages 164–170, 2017.

[17] Erisa Karafili, Linna Wang, Antonis C Kakas, and Emil Lupu. Helping forensic analysts to attribute cyber-attacks: An argumentation-based reasoner. In *International Conference on Principles and Practice of Multi-Agent Systems*, pages 510–518. Springer, 2018.

[18] Erisa Karafili, Linna Wang, and Emil C Lupu. An argumentation-based reasoner to assist digital investigation and attribution of cyber-attacks. *Forensic Science International: Digital Investigation*, 32:300925, 2020.

[19] Hwansoo Lee. Home IoT Resistance. *Telematics and Informatics*, 49, 6 2020.

[20] Leandros Maglaras, Helge Janicke, and Mohamed Amine Ferrag. Cybersecurity of critical infrastructures: Challenges and solutions, 2022.

[21] Fahad Siddiqui, Matthew Hagan, and Sakir Sezer. Establishing cyber resilience in embedded systems for securing next-generation critical infrastructure. In *2019 32nd IEEE International System-on-Chip Conference (SOCC)*, pages 218–223. IEEE, 2019.

[22] Sören Tempel, Vladimir Herdt, and Rolf Drechsler. Towards reliable spatial memory safety for embedded software by combining checked c with concolic testing. In *2021 58th ACM/IEEE Design Automation Conference (DAC)*, pages 667–672. IEEE, 2021.

[23] Robert Thorburn. *Designing a Better Internet of Things, Privacy and Compliance by Design as SysML Domain Extension for Consumer Smart Electronics*. PhD thesis, University of Southampton, 2022.

[24] Robert Thorburn, Andrea Margheri, and Federica Paci. Towards an integrated privacy protection framework for iot: Contextualising regulatory requirements with industry best practices. 2019.

[25] Robert Thorburn, Vladimiro Sassone, Asieh Salehi Fathabadi, Leonardo Aniello, Michael Butler, Dana Dghaym, and Thai Son Hoang. A lightweight approach to the concurrent use and integration of sysml and formal methods in systems design. In *Proceedings of the 25th International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings*, pages 83–84, 2022.

[26] Moritz Weiss and Felix Biermann. Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform*, 26(3):250–267, 2023.

[27] Serena Zheng, Noah Apthorpe, Nick Feamster, and Feamster Chetty. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact*, 2, 2018.

[28] Ruijin Zhu, Baofeng Zhang, Junjie Mao, Quanxin Zhang, and Yu-an Tan. A methodology for determining the image base of arm-based industrial control system firmware. *International Journal of Critical Infrastructure Protection*, 16:26–35, 2017.