PETRAS

Industry Briefing

Cybersecurity for the Internet of Things and Artificial Intelligence at the Intersection Between Digital Infrastructure and Critical National Infrastructure

Dr Monica Racovita

About PETRAS

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 relating to the cybersecurity of IoT devices, systems and networks.

The Centre is a consortium of 22 research institutions and the world's largest socio-technical research centre focused on the future implementation of the Internet of Things. The research institutions are: University College London, Imperial College London, University of Oxford, Lancaster University, University of Warwick, University of Southampton, Newcastle University, University of Nottingham, University of Bristol, Cardiff University, University of Edinburgh, University of Surrey, Coventry University, Northumbria University, Tate, University of Glasgow, Cranfield University, De Montfort University, Durham University, University of Manchester, Royal Holloway, University of London, and University of Strathclyde.

As part of UKRI's Security of Digital Technologies at the Periphery (SDTaP) programme, PETRAS runs open, national level funding calls which enable us to undertake cutting edge basic and applied research. We also support the early adoption of new technologies through close work with other members of the SDTaP programme, such as InnovateUK, supporting demonstrations of new technology and commercialisation processes.

In addition, we build the capacity of the UK to remain a world leader in IoT through our training and development programmes for early career researchers. Finally, we offer consultancy services to the public and private sectors to provide decision makers with insight and advice on a range of cybersecurity related issues.

The wider PETRAS community has played a role in creating this report - in particular Professor Tim Watson from the University of Warwick and Professor Derek McAuley from The University of Nottingham for their critical roles in review, and Emilie Didier and Zakiyya Adam from the PETRAS Business Development Team for their editorial overview.

Design work by Dr Catherine Wheller is based on original work by Dr Michael Stead.

This report should be referenced as follows:

Racovita, M. 2021. Industry Briefing: Cybersecurity for the Internet of Things and Artificial Intelligence at the Intersection Between Digital Infrastructure and Critical National Infrastructure, PETRAS National Centre of Excellence for IoT Systems Cybersecurity, London, UK

DOI:

From the Director

It is my pleasure to present this Industry Briefing on Cybersecurity for the Internet of Things and Artificial Intelligence at the intersection between digital infrastructure and critical national infrastructure. This is the fifth in a series of Industry Briefings, intended to link with and inform the six PETRAS Sectors: Ambient Environment, Supply Chains and Control Systems, Infrastructure, AgriTech, Health and Wellbeing, and Transport and Mobility.

PETRAS has a large network of industry partners and expert academics, and works directly in collaboration with these and government partners to ensure that research can be directly applied to benefit society, business and the economy. I am delighted to see that as a Centre dedicated to identifying and addressing some of the needs within IoT, PETRAS has managed to connect industry with social and physical scientists to work towards some of the major challenges and questions around the cybersecurity of the Internet of Things. As IoT technology develops at speed and embraces AI and machine learning 'at the Edge', so do the challenges around cybersecurity and systems, and it is critical that these are addressed by industry, government and academia.

We hope that these Industry Briefings, which have highlighted insights into the challenges of deploying IoT systems, provide a fresh perspective on the existing and emerging opportunities for industry and those working within the Transport and Mobility sector. With exciting innovative ideas, we are positive that PETRAS will be able to encourage collaboration between academia and industry, supporting the opportunities these challenges present, and we look forward to opening these discussions.

I hope this Industry Briefing will catalyse further debate and collaboration between researchers and users, making the use of the IoT safe and trustworthy, and maximising its social and economic value to the UK.

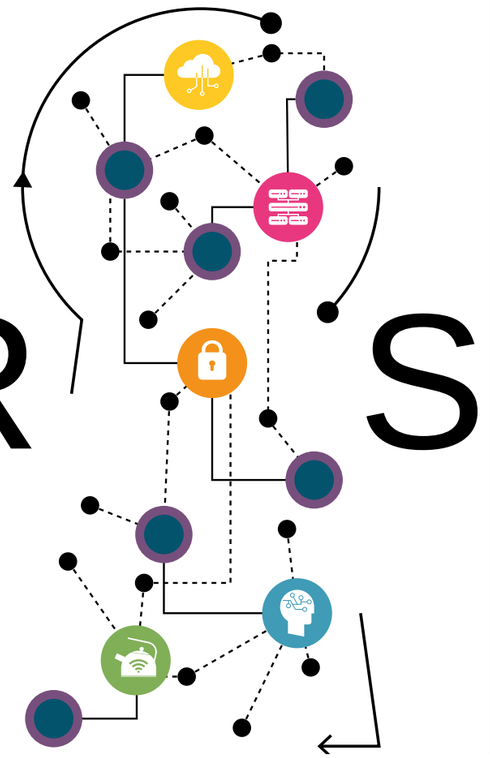
Professor Jeremy Watson CBE FREng
Director of the PETRAS National Centre of Excellence

UKRI Engineering and Physical Sciences Research Council

Contents

PETRAS

THE PETRAS NATIONAL CENTRE OF EXCELLENCE FOR IoT SYSTEMS CYBERSECURITY



Executive Summary

The digital infrastructure supporting Internet of Things (IoT) and Artificial Intelligence (AI) is increasingly designated as part of Critical National Infrastructure (CNI), thus transforming some of the IoT and AI security vulnerabilities into CNI vulnerabilities.

While the main approach to digital/ CNI security in general has focused on preparedness and resilience measures, new approaches argue for the need to be proactive and focus on vulnerability treatment. IoT represent a significant risk for CNI through their high and increasing numbers and increased opportunities for attacks.

AI in cybersecurity has a dual-use nature: it can aid in cybersecurity protection through the detection of malicious patterns and behaviours but may also be used for malicious purposes.

The main challenges faced by IoT and AI in digital infrastructure/CNI include:

Policy:

- High fragmentation of digital security regulatory requirements worldwide, government intervention vs 'laissez-faire' approach is too simplistic for increasing the digital security of products
- Security gaps often due to economic factors
- Challenges to cyber resilience
- Increased interconnectedness and interdependencies between systems
- CNI ownership

Technical research:

- Shortage of cyber skills
- Modelling interdependencies
- Vulnerabilities and risks
- AI cybersecurity (automatic formal verification and validation, explainability and transparency, novel security techniques to counter emerging AI threats)
- 5G (achieving a balance between ease of connectivity and security, facilitate different types of network configuration, manage a high density of connected devices etc.)

Socio-technical issues:

- Geopolitics (in particular geopolitical dispute between China and the US)
- Privacy and data protection

Possible new research and innovation opportunities in IoT and AI cybersecurity could include AI and specifically machine learning (ML) techniques in combination with edge computing for control and analytics, IoT security measures that would balance device limitations, active cyber defence such as deception based cyber defence, and isolated IoT identity.

Introduction

Scope of this brief

The current industry brief offers a summary of the general trends, challenges and opportunities in cybersecurity and associated policy for the Internet of Things (IoT) and Artificial Intelligence (AI) in the digital infrastructure part of the Critical National Infrastructure (CNI). It reviews the most recent developments in the field concerning the UK, EU and globally relevant trends up to the publication date of this brief. The brief concludes with insights into UK research landscape activities and business development opportunities with PETRAS.

The brief is constructed as a primer for discussion, and the target audiences for this brief include:

- government organisations involved in digital infrastructure part of the critical national infrastructure,
- companies that provide IoT solutions to the that part of the sector,
- companies that provide cybersecurity solutions to IoT,
- companies looking for cybersecurity solutions, and
- researchers involved in the digital and critical infrastructure cybersecurity sector, interested in collaboration opportunities with PETRAS.

In this document, IoT devices are interpreted as components of an ecosystem, along with data communication, data-aggregation and -processing, data analytics and data visualisation. AI is concerned as long as it applies to edge computing. Two UK based cybersecurity experts provided feedback included in this brief: Expert A (academia) and Expert H (private sector).

Sector background

IoT devices such as smart meters, pet trackers, or self-driving vehicles are only one layer of a complex ecosystem which represents the IoT value chain. Aside from the devices themselves, which comprise sensors and actuators and communications hardware, the IoT value chain includes the connectivity network (cellular, fixed or satellite), backend systems (servers in the cloud or on site collecting and analysing data), software platforms (for device management, security and data analytics), billing and customer support, and system integrators (SIs) or developers[1]

The deployment of IoT is predicted to increase in combination with 5G and edge computing to allow for real-time processing, and in combination with data analytics and AI[2]. The growth of IoT will also allow a higher connectivity within and between industry sectors. These trends are increasingly linked with to the so-called 4th industrial revolution or Industry 4.0 which "comprises advanced manufacturing technologies that capture, optimise, and

deploy data" [3]. Yet, European Institute of Innovation and Technology (EIT) experts say, lack of standards and business models will prove higher obstacles than lack of capital. Another potentially worrisome aspect is the protection of data gathered by IoT[2].

However, many business owners seem reticent about a large-scale deployment of IoT due to a misunderstanding of digital transformation, as they perceive it as a piecemeal or an add-on change, rather than redefining value creation[4]. Such business owners see multiple challenges associated with the adoption of IoT in industry (Industrial Internet of Things-IIoT)[4] such as massive data generation, worker displacement, complete replacement of legacy equipment, being 100% ready for digital transformation, costly continuous improvement, and lack of feasibility in emerging economies. Yet, seeing it as a redefinition of value creation, Lauritzen et al argue[4], all these challenges could be turned around to be manageable issues and even points of strength.

On the downside of an increase use of IoT/IIoT, the combination with 5G and cloud computing would mean an increase in attack surfaces and vulnerabilities[2]. For IoT/5G/cloud computing part of CNI particularly worrisome are increases in in international attacks (state-sponsored or not), as well as having an increased reliance on third country suppliers[2] . For companies, digitalisation can bring both cyber risks and cyber threats, according to a McKinsey article[5]. The authors explain that cyber threats can lead to loss of confidentiality, integrity, and availability of digital assets, while the risks brought by these threats can results in fraud, financial crime, data loss, or loss of system availability. Current cybersecurity approaches for companies focus on a maturity-based cybersecurity approach, which includes approaches such as security operations centres, multifactor authentication, and can generate a growth of control and oversight that can become unmanageable. A risk-based approach, Boehm et al argue[5], will focus and prioritise funds for the worst vulnerabilities and most significant threats.

A 2020 PwC global survey with more than 3000 business, technology and security executives indicates an increase of the role of and investments in cybersecurity: half of respondents (up 25% from previous year) said they consider cybersecurity for every business decision, and 55% plan to increase cybersecurity budgets even though they expect revenues to decrease[6]. In terms of threats the respondents indicated:

- IoTs to be the threat vectors with the highest likelihood and impact
- the state sponsored attacks on critical infrastructure to have the lowest likelihood
- successful attacks from cyber criminals to have the highest likelihood and the highest impact.

The highly interconnected nature of IoT and AI at the edge as well as their complex relationships with various elements of CNI has increased the appeal of AI to be used not just to detect malicious patterns and behaviours but also for malicious purposes (for larger scale and more powerful attacks)[7].

Internet of Things and AI Cybersecurity

Attacks and vulnerabilities

Some of the main types of attacks in digital infrastructure include[8]:

- **Distributed denial of service (DDoS)** (a type of attack in which an online service is flooded with illegitimate requests) remains common but large scale incidents are rare
- Phishing (obtain sensitive information by disguising as a trusted online entity) and farming (redirected to websites that ask for personal information) remain high and are increasingly difficult to detect
- **Ransomware attacks** (a type of digital extorsion) are becoming more targeted; they can paralyse the physical operations of the cyber-physical systems such as IoT; the most famous such attacks were WannaCry and NotPetya and together caused billions of dollars of damages
- **Malware** is becoming more sophisticated, evading detection and targeting new technologies. One example is fileless malware which is executed in the user's browser and does not leave any trace on the hard drive.

The main approach to digital security has focused on threats, incident response and impact reduction (preparedness and resilience measures). Yet, OECD argues that it is better to be proactive (placing the focus on vulnerability treatment) than reactive, as the current main approaches are[9].

The vulnerability treatment lifecycle includes[9]:

- **Discovery:** when a vulnerability is found, it needs to be reported to the 'vulnerability owner,' the organisation with the responsibility to mitigate the vulnerability.
- **Handling:** the 'owner' needs to develop a solution and distribute it to all users if it is a code vulnerability.
- **Management:** if the vulnerability is in an information system, the 'system owner' needs to find a solution, e.g. apply a patch, change the system or reconfigure the product.
- **Disclosure:** directly concerned parties (the public or security community) need to be informed about the vulnerability to develop security tools and enhance the community's knowledge.

The OECD report on vulnerability treatment lifecycle further states that the vulnerability lifecycle is often a race against time, and ideally all stakeholders involved, vulnerability owners, code owners, system owners and security researchers, need to understand their role and assume responsibility. Sometimes even if vulnerabilities are detected, some organisations have long patching delays or even no patching because it would interrupt vital assembly lines or physical processes. Patching vulnerabilities can also be an expensive and complex process. If an organisation manages to get past these challenges it can face higher level ones

researchers, with or without incentives like rewards. Grey markets are partially regulated (may be legal or illegal, depending on the jurisdiction and context), and sellers are often not the vulnerability owners and buyers are not necessarily aiming to fix the vulnerability. Players can be government intelligence and defence agencies, companies developing and selling security tools. Black markets are illegal, and take place on underground and anonymous platforms in the dark web[9].

Although all products that contain code also contain vulnerabilities even in a security-by-design approach, not all vulnerabilities are

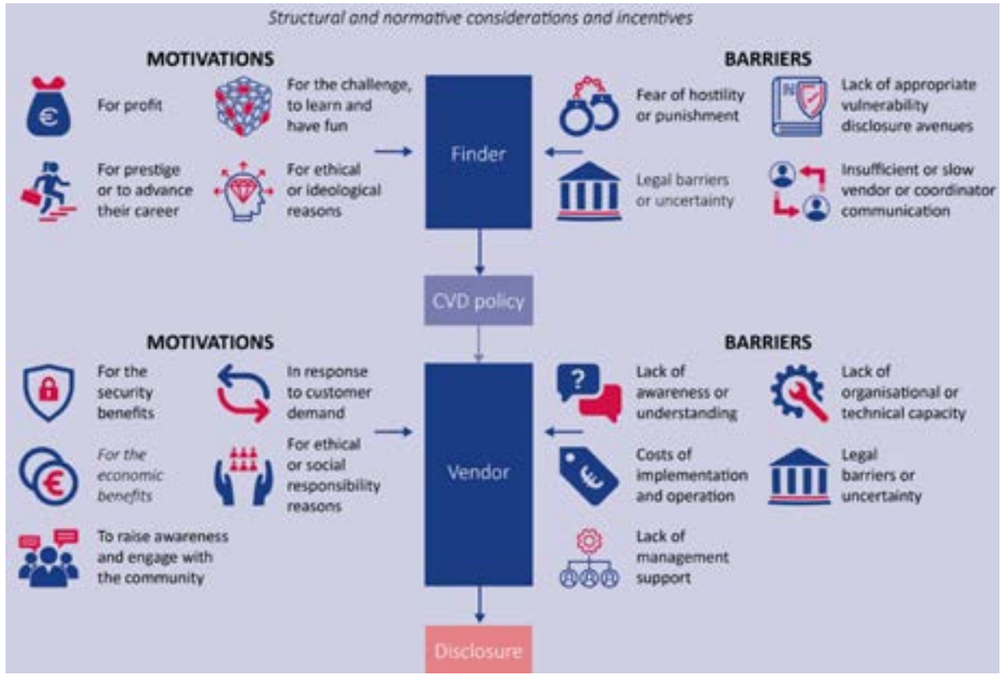


Figure 1. A coordinated vulnerability disclosure process[10]

such as the grey and black markets for vulnerabilities, and limited trust in the government[9].

Vulnerabilities can be exchanged through white, grey or black global markets. The white markets are regulated markets that connect vulnerability owners and

critical and not all are easily exploitable[8]. Veracode estimates that approx. 13% of all vulnerabilities are critical (attacks are straightforward and they can compromise servers or infrastructure)[11].

In some cases, attempts to fix vulnerabilities, even in the case of an attack can prove to be controversial. For example, during the WannaCry attack Microsoft decided, as a result of public pressure, to provide a security update to products that have reached their end-of-support/end-of-life (EOL). While some experts criticised the move as encouraging consumers to use products beyond the end of commercial support, other consider that the source code for products that reach their end-of-support should become public domain[8].

Overall, many stakeholders do not have incentives to uphold and take responsibility for digital security, for the industry due to the need to save time and costs and for the consumers due to placing higher value on usability and price[8].

Efforts to increase the security for IoT include security labels, either as partnerships between the government and industry (Finland), voluntary labelling from business associations (Japan), or as a governmental labelling scheme (Germany), as well as mandatory guidelines for IoT security (UK and Japan)[8].

As part of CNI, IoT and underlying

digital infrastructures can face new and technologically sophisticated threats, many with a geopolitical dimension, categorised as cyber crime, cyber terrorism, cyber espionage and cyber warfare[12]. Organised cyber crime entities are getting better at using the resources of the dark web and collaborating with one another, as well as escaping prosecution, with cyber crime-as-a-service increasing as a business model, says a World Economic Forum (WEF) report[13].

The WEF publication further reports that an estimated number of 21 billion IoT devices in use worldwide is set to double by 2025. With a sustained increase in attacks (300% increase in the first half of 2019 compared to the previous year; IoT used to take down Wikipedia in September 2019), IoT are a particular cybersecurity concern for CNI. Damages caused by attacks done using IoT are predicted to amount to USD 6 trillion (GBP4.3 trillion) (almost equivalent to the GDP of 3rd largest economy.

To tackle vulnerabilities in IoT, some researchers[14] suggest that standards for IoT devices should focus on four security domains and eight goals as presented in Figure 2.

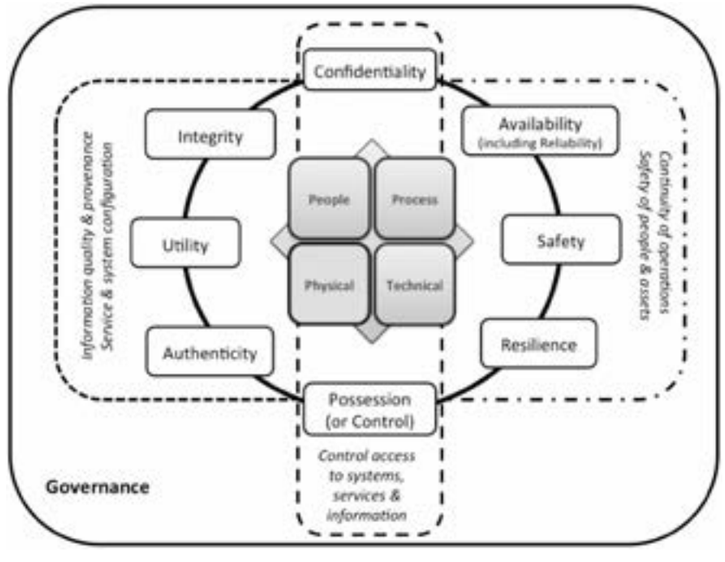


Figure 2. Security domains and goals for IoT devices[14]

A particular security issue is the use of information represented as data, expert H consulted for this brief mentioned. At times, the expert indicates, data can represent hidden risks as “not even the organisations themselves know where their information is or how they depend on each other”. In addition, “data centres and related data services are not currently designated CNI but (I would argue) all the UK’s CNI depends on them in ways that haven’t been analysed (yet). Of course, society and government also depend on this data infrastructure too”.

Artificial intelligence

As for AI, its role in digital/CNI security can be multifaceted:

- Having the potential to aid in cybersecurity protection through the detection of malicious patterns and behaviours. Currently deployed AI in cybersecurity includes uses in anomaly detection and identifying novel phishing attacks[15]. Potential use of AI has been indicated for response and recovery as part of cyber resilience[16].
- Be the target of malicious attacks. Attackers can try to take control of AI (a difficult option) or try to influence its decisions by manipulating inputs, known as adversarial Machine Learning (e.g. by making small changes to digital images that are undetectable by humans) or data poisoning (introducing inaccurate data)[17]. In addition, if datasets contain sensitive or personal information there are additional issues to consider like transparency and accountability[17].
- Be used for malicious purposes. Kaloudi and Li identify five categories of AI-based cyberattacks: next generation malware, voice synthesis, password-based attacks, social bots, and adversarial training[17].

A 2018 joint report authored by world experts in AI safety, drones, cybersecurity, lethal autonomous weapon systems, and counterterrorism following a workshop at the University of Oxford, emphasises the dual-use nature of AI in cybersecurity and recommends to researchers and policy-makers to adopt best practices in recognition of this trait (including better communication and higher responsibility) [18]. The authors also predict a change in the threat landscape due to an increased use of AI: an expansion of existing threats due to lower costs of AI, introduction of new threats due to AI performing tasks otherwise difficult or impractical for humans, and a change to the typical character of threats (more effective, better targeted).

Challenges

Policy

OECD indicates that the high fragmentation of digital security regulatory requirements worldwide represents a challenge for industry (high costs, interoperability issues) and policy-makers[19]. International cooperation in cyberspace, also recommended by the US Cyberspace Solarium Commission, the US intergovernmental body advising on defence against cyberattacks[20], among all stakeholders and all components of the value chain and with clear allocation of responsibility, is key to address cybersecurity. To achieve efficient cooperation, governments need to put in place instruments to ensure trustworthiness as “the ability of suppliers to meet the expectations of a contract partner in a verifiable way”[19].

The OECD also argues that the dichotomy of government intervention vs ‘laissez-faire’ approach is too simplistic for increasing the digital security of products and that many policy options lay in between[19]:

- Raising awareness of mainstream users and developing digital security skill
- Lead by example (public procurement policies, patching of vulnerabilities)
- Technical standards and voluntary frameworks
- Labels
- Ex post mechanisms (requires a review of existing frameworks)
- Ex ante regulations (from technical requirements to high level principles).

According to the report by OECD, security gaps often exist/emerge due to economic factors, such as insufficient market incentives; information asymmetries and externalities; unclear allocation of responsibility; and lack of cooperation among stakeholders[19]. Together, the report states, these factors lead to a lack of adherence to voluntary guidelines and standards, including security-by-design and security-by-default. In addition, another looming policy challenge is posed by the growth of “Internet of forgotten things”, products in the EOL gap, still in use but with no security support[19].
In response to these challenges, OECD proposes six high-level principles to enhance the digital security of products[19]:

1. Increasing transparency and information sharing
2. Raising awareness and empowering stakeholders
3. Ensuring responsibility and duty of care for supply-side actors
4. Increasing cooperation among all stakeholders
5. Promoting innovation and competition
6. Addressing digital security with proportionality, through a risk-based approach.

Yet, when part of CNI, IoT devices and their digital infrastructure must often go beyond security towards assuring resilience. In Humphreys' view, this is representative of "a global trend among developed countries toward CI policies favouring society-centric resilience at the system level over security-oriented protection of specific assets deemed at risk"[21].

In the UK, the creation of NCSC as well as introducing security regulation for some CNI sectors (civil nuclear and financial), as well as the implementation of the European NIS Directive are indicated as good initiatives for boosting resilience[22], but the continuing reliance on market forces for building CNI resilience has been criticised[22]. Challenges to cyber resilience include lack of a regulator with statutory powers for some CNI sectors; a fragmented regulatory landscape further complicated by joint Competent Authorities; and mixed capacity among regulators to ensure appropriate support.

OECD draws attention to the challenge of increased inter-connectedness and inter-dependencies between systems and between different countries. These independently and together increase the impact of cyberattacks and natural disasters, both major sources of vulnerability for CN[23]. In addition, OECD states that the rise of 'smart infrastructures', like smart cities or autonomous vehicles, could bring additional challenges to resilience that are not completely understood.

Another challenge for policy is the ownership of CNI. In many Western countries the greatest part of CNI is privately owned. Early governance models, thus, relied on voluntary collaborations between the public and private sectors. Risk management also relied on "incentives, information sharing, and voluntary investments in security"[21]. This can sometimes make difficult assigning responsibilities for investment costs or design regulations. In the UK, as the National Security Strategy 2016–2021 found, relying on voluntary measures is not enough; they need to be supplemented by mandatory regulations[24].

Technical Research

Shortage of cyber skills

Cyber skills are a critical element of the digital/CNI cybersecurity[25]. At global level the shortage of cyber skills is a well-known challenge. Yet, recent developments, some due to the global pandemic according to some sources[26], see a significant decrease in the cybersecurity skill shortage.

In addition to increasing specialised cyber skills, expert A consulted for this brief pointed out that in many circumstances a greater security awareness is needed from non-specialists.

Modelling interdependencies

Identifying, understanding and analysing inter-dependencies among different components and sectors in CNI is a major challenge for governments, as highly complex systems can see severe consequences even for small disruptions[12]. As digital infrastructures are increasingly linked with all other infrastructures, Sharma argues, it becomes increasingly difficult to separate critical from non-critical elements[12].

To add another layer of complexity, infrastructures are socio-technical systems that have then both physical and social elements. For the latter, human actors have "different, possibly conflicting, interests and, hence, different perceptions of 'reality'" [27]. Yet, as expert A indicated, high complexity does not necessarily make modelling impossible. A possible issue, however, the same expert says, when such a model is made it can be used as a tool to either plan or rehearse an attack on CNI.

Current modelling approaches are categorised as follows[28]:

- **Empirical:** use of past accident or disaster data to analyse interdependences, can identify common failures and attack patterns, but require large amounts of data
- **Agent-based:** create complex models from looking at simpler agents and their behaviour, it can be used to study interdependencies between agents and effects of failures or attacks, but the accuracy of the model depends on the accuracy of the agents used
- **System dynamics:** use feedback loops to identify connections and direction of effects, it allows the identification of mitigation measures for particular risks (like epidemics), but can require large amounts of data which cannot be accessed due to security concerns and cannot analyse component-level dynamics
- **Network-based:** infrastructures are seen as networks in which the nodes are CNI components, yet cannot provide enough information on flows
- **Economic theory based approaches:** interdependencies are modelled using input–output and computable general equilibrium, and are used for macroeconomic or industry level interdependencies, but they cannot provide an analysis at the component level and the interdependence strength is measured only in normal economic situations.

A promising approach, in terms of outputs and integration, is seen in the High Quality Data Modelling (HQDM) approach[29], which is central to the work conducted on the new UK National Digital Twin Programme [30].

Vulnerabilities and risks

Digital infrastructure security has focused on threats, incident response and impact reduction (preparedness and resilience measures). Yet, new developments, summarised by OECD, argue that it is better to be proactive (placing the focus on vulnerability treatment) than reactive, as the current main approaches are[9].

An ENISA report further investigated the economics of vulnerability disclosure and found that there is a need for systematic research on the motivations of finders, how to better quantify the cost of the exploitation of vulnerabilities, the cost of implementing and running vulnerability disclosure programmes, the quantification of security gains through vulnerability disclosure, and the cost of developing and implementing patches[10].

AI

The use of AI in CNI cybersecurity looks like a promising domain. A few examples are the use of Deep Learning methods to develop generalised models[31], identification of insider threats[32], attack-detection in IoT critical infrastructure[33].

At the same time, AI can be misused by malicious actors to conduct attacks or introduce new security vulnerabilities inherent to the technology itself. ENISA indicates that further research is needed to address various gaps in the use of AI in cybersecurity, such as "automatic formal verification and validation, explainability and transparency, novel security techniques to counter emerging AI threats"[34].

5G

5G enabled IoT has been receiving a lot of attention for the past few years regarding adoption and standardisation, spectrum requirements, as well as the actual implementation of the 5G technology as

opposed to the initial promises (including issues with transmission/reception, interference, low latency)[35]. For 5G to enable IoT the challenges include, according to Shafique and collaborators[35]:

- Achieving a balance between ease of connectivity and security
- Facilitate different types of network configuration
- Manage a high density of connected devices
- Coverage enhancement to support tactile internet and multimedia applications
- Energy efficiency

Socio-technical

Geopolitics of CNI

A 2017 BT white paper argues that the most serious threats in CNI cybersecurity come from organised crime or foreign government hacking[36]. “Strategic economic advantages, political gains and traditional espionage objectives” can motivate governments to engage in cybersecurity attacks on other CNI, states BT.

CNI security concerns regarding China’s Digital Silk Road and Chinese digital investments in Western CNIs in a context of a heightened geopolitical dispute between China and the US have been raised[37]. Countries that have security alliances with the US but are also the recipients of Chinese digital infrastructure need to find a balance between commercial and security interests and thus have difficulties choosing one side or the other, the report finds.

A case in point and possibly an escalation of this issue is the example of Huawei and its involvement with 5G networks around the world. On May 2020 US government announced a banning of selling American system components, vital for the company, to Huawei based on concerns that “mobile networks which rely on Huawei could allow snooping and sabotage by China”[38].

Other countries like Australia, Canada and Singapore followed suit and banned Huawei 5G equipment. Europe, including the UK, has a more complicated relationship with both the US and China, in the context of which both US and China are economic partners but also competitors. European societies need to capitalise on the 5G wave as quickly and as profitably as possible, maintain consumer’s best interest in mind, deal with a values dilemma (doing business with powers driven by opposite values), maintain technological autonomy, and juggle national/regional defence priorities [38].

The World Economic Forum Global Risks Report 2020[13] lists among the most important geopolitical risks for digital innovation:

- **lack of a global tech governance framework**, influences standards, “the foreign participation in national critical infrastructure, foreign acquisition of domestic technology, the offshoring of data, and technology transfer as a price to access foreign markets, influencing societal risks as well” (in the social risks category being digital divide and wealth gaps, biased algorithms and cyberbullying, workplace surveillance and employee privacy);
- **rise of geopolitical tensions**, which increases risks and minimises cooperation;
- **parallel cyberspace**, a possible divergence of internationally established protocols as well as the pursuit of “cyber-sovereignty” could lead to lead to the fragmentation of cyberspace
- **first-mover advantage**, patents on breakthrough technologies can shift geopolitical balance
- **a new digital arms race**, digitalisation raises three critical issues: “how to protect critical infrastructure, uphold societal values and prevent the escalation of state-on-state conflicts”; it also increases the risk of asymmetric war empowering smaller countries and state actors.

Privacy and data protection

The General Data Protection Regulation (GDPR) of the EU, which came into force in 2018, is perhaps one of the most comprehensive legal framework concerning the protection of personal data in the world. It has constrained the processing of personal data based on seven principles: lawfulness; fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and added new obligations with regards to accountability. It also introduces the ‘right to be forgotten’ and the data portability right to enable citizens’ control of their own data[39].

Opportunities

Industry 4.0 is set to become more than a buzzword, with projections for smart factories to bring in 215 billion USD (154 billion GBP) by 2025 and 10–15 trillion USD (7-10 trillion GBP) globally over the next 20 years[40]. Aside from revenues, IoT and communication technologies are reported to increase communication efficiency within factories, among different departments, and outside with suppliers and customers. These technologies can also optimise performance and conduct predictive maintenance[40].

Among the concerns, cybersecurity comes at the top. While there are many cybersecurity challenges facing IoT and AI as presented in section 3, of this document, some authors also mention research and innovation opportunities in this area[41]:

- Within the context of blockchain technology, private blockchains and zero-trust networks (participants in the blockchain by default do not trust each other and verify each other's identities)
- Within AI, and particularly ML domain, connected to edge computing and IoT, AI and specifically ML can be used to better analyse cyber behaviours, identify threats and vulnerabilities and detect attacks
- Lightweight IoT security, as security for IoT devices needs to strike a balance between security needs and limited power and memory
- Active cyber defence, such as deception-based cyber defence, as opposed to passive traditional cyber defence mechanisms, such as such as encryption, authentication and access control. Examples of active cyber defence include address hopping, honeypots and network telescopes
- Isolated IoT identity and giving internet devices other addresses than IP, isolating devices from the outside world and only allowing connections through cryptographic keys.

PETRAS in the UK Research Landscape

UK research institutes conducting work on cybersecurity/IoT:

- Research Institute in Sociotechnical Cyber Security (RISCS), working on human behaviour and cybersecurity, understanding and assessing cybersecurity evidence, ransomware[42]
- Research Institute in Verified Trustworthy Software Systems (VeTSS), working on formal verification[43]
- Research Institute in Trustworthy Inter-Connected Cyber-Physical Systems (RITICS), working on Integration/adoption of agile methods and techniques to traditional processes/ systems (transition), verification, NIS directive, justification framework, human behaviour and cybersecurity[44]
- Research Institute for Secure Hardware & Embedded Systems (RISE), working on open source platforms, device (hardware) and platform security (Verification), secure user interaction, trustworthy design[45]
- Centre for Research and Evidence on Security Threats (CREST), working on human behaviour and cybersecurity, IoT (smart homes)[46].

In addition, some of the most important testbeds in the UK (according to Hankin, 2018[48]) are:

- MUMBA (Multi-faceted Metrics for ICS Business Risk Analysis) project at the University of Lancaster, completed in 2017[48]
- The Infrastructure Transitions Research Consortium (ITRC) is a consortium of 7 universities (Cambridge, Cardiff, Leeds, Newcastle, Oxford, Southampton and Sussex). Within it the Data and Analytics for National Infrastructure (DAFNI) project aims to create a national infrastructure database for visualisation and analysis.[49]
- UK Collaboratorium for Research in Infrastructure & Cities (UKCRIC) is an integrated research capability for a UK-based national infrastructure research community. To date, phase I has funded 13 cross-disciplinary lab and urban observatory test facilities which provide data to be used for policies, regulation, investments and strategic decisions.[50]
- The University of Bristol's cybersecurity testbed provides a realistic environment for researching cyber-physical systems[51].

Table 1. Past PETRAS projects in cybersecurity in infrastructure/IoT cybersecurity

Project	Partners	Description	Industrial relevance
Potential Impact of IoT Boosted Botnet Attacks (BotThings)	National Cyber Crime Unit (Supported by Lloyd's Register Foundation)	Observe current botnets to simulate potential future botnet threats and study vulnerabilities in devices (botnet: a network of bots; bot: software application that runs automated tasks over the Internet)	Healthcare, higher education, energy, small and medium-size industries
Security Risk Assessment of IoT Environments with Attack Graph Models (SECRIS)	Building Research Establishment	Design a new generation of attack graph (succinct representation of all paths through a system that end in a state where an intruder has successfully achieved his/her goal). Models capable of describing the attack surface of modern IoT infrastructure for smart building	Smart buildings
Developing a Consumer Security Index for Consumer IoT Devices (CSI)	Department for Digital, Culture, Media, & Sport, UCL Dawes Centre for Future Crime, Home Office, Which?, IBM, The Behavioural Insights Team, MOPAC	Review security features currently provided for consumers; review crime prevention message in IoT manuals; develop a consumer security index for consumer IoT devices; encourage the use of the index for retailers	Smart homes, wearable medical devices
Developing a Consumer Security Index for Domestic IoT Devices Plus (CSI+)	DCMS, IBM Software, MOPAC, BRC	Provide a clear picture of the security of domestic IoT devices, including producing a consumer security index for public use; synergy with PETRAS Cyberhygiene project	Smart homes, wearable medical devices
The Internet of Energy Things (P2P-IoET)	Siemens, UKPN	Lay the grounds for collaborative economic business models in energy; analyse the regulatory, security, engineering and social requirements for their acceptability	Energy industry
Cyber Risk Assessment for Coupled Systems (CRACS)	Fujitsu Labs Europe, NSC	Identify new risks in coupled systems and explore the development of new methodologies by working with multiple stakeholders	Social media, any industry using IoT to provide services to consumers
Blockchain-empowered Infrastructure for IoT (BlockIT)	Centrica (British Gas), DSTL	Investigate how blockchain can make infrastructure for IoT more resilient and guarantee integrity and privacy	Energy

Table 1 cont. Past PETRAS projects in cybersecurity in infrastructure/IoT cybersecurity

Project	Partners	Description	Industrial relevance
Analytical Lenses for IoT Threats (ALIoTT)	Network Rail, Highways England, Singapore Land Transport Authority, Home Office, CPNI, Public Health England, DSTL, Costain, Siemens, BT, Telefonica, EE	Develop tools to analyse different threats in a wide array of infrastructural and service deployment contexts	Transport, health, telecommunications
Cyberhygiene	BBC, Which?, Sogeti, CESG	Better understanding of what factors influence individual and corporate user's behaviour for actions that can mitigate risks from cyber attacks	Any industry at risk of cyberattacks
IoT Multi-disciplinary Standards Platform (IoT-MSP)	GCHQ, IET standards group, IoTUK, Digital Catapult	Develop the concept of an IoT Multi-Disciplinary Standards Platform, to exploit research outputs from PETRAS	Any industry using IoTs
IoT Observatory	--	Sharing IoT datasets on a large distributed scale to support innovation, by not compromising privacy and security	Any industry handling data sets
Home Area Network Code of Practice (HANCODE)	EDF Energy	Develop a code of practice to be adopted by energy suppliers and manufacturers of devices that link smart meter home area network and consumers; identify technical and security issues	Energy industry
Self-Sustained Blockchain-based Treasury System (BTS)	Input Output HongKong Ltd	Model, design and implement a secure treasury systems compatible with blockchain infrastructure	Any industry using blockchain (e.g. finance)
Resilience and Security in Low Power IoT (RSIOT)	IBM UK	Address security concerns for low power sensors with long range communication; create a network of such sensors that would increase resilience and security protecting against denial of service attackers	Energy management, natural resource reduction, pollution control, infrastructure efficiency, disaster prevention

Table 1 cont. Past PETRAS projects in cybersecurity in infrastructure/IoT cybersecurity

Project	Partners	Description	Industrial relevance
IoT in Control	BRE, Cube group, CESG	Explore vulnerabilities that exist in industrial and building control systems	Smart buildings, sensors, industrial control systems
Hybrid Engagement Architecture Layer for Trusted Human-Centric IoT (HEALTH-I)	CityVerve, Southampton City Council, Zooniverse	Integrate humans into IoT ecosystems using crowdsourcing to improve trust of devices (openly and transparently)	Retail, medical, logistics, transportation
National and International Policy for Critical Infrastructure Cybersecurity (NIPC)	Network Rail, Highways England, US Transportation Research Board (NAS), EU Mobility & Transport, Singapore Land Transport Authority, Home Office, CPNI, DSTL, GLA, RBS, Costain, Siemens, BT, Telefonica, EE, TRL	Compare and contrast approaches to manage IoT threats from a policy perspective	Transport networks, communication networks
Security and Performance in the IoT Smart Home (SPIoTSH)	The Internet of Things Security Foundation (IoTSF) and the Building Research Establishment (BRE)	Develop a reference architecture that facilitate security analysis of smart home components and relates this to real-world smart homes	Smart homes

PETRAS has a dedicated Business Development team who connect the public and private sectors with a network of transdisciplinary academic experts, to enable research collaborations that address social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

If you are a research institution, private or public sector organisation interested in collaborating with PETRAS, please contact petras@ucl.ac.uk.

Abbreviations

AI (Artificial Intelligence)

CI (Critical Infrastructure)

CNI (Critical National Infrastructure)

ENISA (European Union Agency for Cybersecurity)

EOL (End of life)

IoT (Internet of Things)

IIoT (Industrial Internet of Things)

ML (Machine Learning)

OECD (Organisation for Economic Co-operation and Development)

NCSC (UK's National Cyber Security Centre)

WEF (World Economic Forum)

End Notes

[1] M. Mackenzie and T. Rebbeck, ‘What is the IoT value chain and why is it important?’, Analysys Mason, Oct. 06, 2020. https://www.analysysmason.com/research/content/comments/iot-value-chain-rdme0/ (accessed Mar. 01, 2021).

[2] EIT Digital, ‘New report on European digital infrastructure and data sovereignty’, European Institute of Innovation & Technology, Jun. 2020. Accessed: Jan. 11, 2021. [Online]. Available: https://eit.europa.eu/news-events/news/new-report-european-digital-infrastructure-and-data-sovereignty

[3] BCG, ‘Industry 4.0’, BCG Global. https://www.bcg.com/capabilities/manufacturing/industry-4.0 (accessed May 17, 2021).

[4] M. Lauritzen, D. Lee, M. Lehnich, and K. Liang, ‘Industrial IoT generates real value—if businesses overcome six myths’, McKinsey Our Insights, Jun. 02, 2020. https://www.mckinsey.com/business-functions/operations/our-insights/industrial-iot-generates-real-value-if-businesses-overcome-six-myths (accessed Jan. 11, 2021).

[5] J. Boehm, N. Curcio, P. Merrath, L. Shenton, and T. Stähle, ‘The risk-based approach to cybersecurity’, McKinsey Our Insights, Oct. 08, 2019. https://www.mckinsey.com/business-functions/risk/our-insights/the-risk-based-approach-to-cybersecurity (accessed Jan. 12, 2021).

[6] PwC, ‘Global Digital Trust Insights Survey 2021’, Pricewaterhouse Coopers, 2020. Accessed: Jun. 16, 2021. [Online]. Available: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/assets/pwc-2021-global-digital-trust-insights.pdf

[7] N. Kaloudi and J. Li, ‘The AI-Based Cyber Threat Landscape: A Survey’, ACM Comput. Surv., vol. 53, no. 1, p. 20:1-20:34, Feb. 2020, doi: 10.1145/3372823.

[8] OECD, ‘OECD Digital Economy Outlook 2020’, OECD Publishing, Paris, Text, 2020. Accessed: Mar. 02, 2021. [Online]. Available: https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2020_bb167041-en

[9] OECD, ‘Encouraging vulnerability treatment: Overview for policy makers’, OECD Digital Economy Papers, vol. 307, Feb. 2021, doi: https://doi.org/10.1787/0e2615ba-en.

[10] E. Silfversten, W. Phillips, G. P. Paoli, and C. Ciobanu, ‘Economics of Vulnerability Disclosure’, ENISA, Report/Study, 2018. Accessed: Mar. 04, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

[11] Veracode, ‘The State of Software Security Today Volume 9’, Veracode, Burlington, Massachusetts, 2019. [Online]. Available: https://www.veracode.com/sites/default/files/pdf/resources/reports/state-of-software-security-volume-9-veracode-report.pdf

[12] M. Sharma, ‘Securing Critical Information Infrastructure: Global Perspectives and Practices’, Institute for Defence Studies and Analyses, New Delhi, India, 60, Apr. 2017. [Online]. Available: https://idsa.in/system/files/monograph/monograph60.pdf

[13] World Economic Forum, ‘The Global Risks Report 2020’, World Economic Forum in collaboration with Marsh & McLennan and Zurich Insurance Group, 15th edition, 2020. Accessed: Mar. 19, 2021. [Online]. Available: https://wef.ch/3aiRxl5

[14] H. Boyes and T. Watson, ‘Towards a secure and resilient IoT architecture for smart home energy management’, in Living in the Internet of Things (IoT 2019), May 2019, pp. 1–7. doi: 10.1049/cp.2019.0161.

[15] National Academies of Sciences, Engineering, and Medicine, Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop. National Academies Press, 2019.

[16] A. Kott and P. Theron, ‘Doers, Not Watchers: Intelligent Autonomous Agents Are a Path to Cyber Resilience’, IEEE Security Privacy, vol. 18, no. 3, pp. 62–66, May 2020, doi: 10.1109/MSEC.2020.2983714.

[17] J. Wolff, ‘How to improve cybersecurity for artificial intelligence’, Brookings, Jun. 09, 2020. https://www.brookings.edu/research/how-to-improve-cybersecurity-for-artificial-intelligence/ (accessed Mar. 04, 2021).

[18] M. Brundage et al., ‘The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation’, arXiv:1802.07228 [cs], Feb. 2018, Accessed: Apr. 30, 2021. [Online]. Available: http://arxiv.org/abs/1802.07228

[19] OECD, ‘Enhancing the digital security of products: A policy discussion’, OECD Publishing, Paris, 306, Feb. 2021. Accessed: Feb. 19, 2021. [Online]. Available: https://www.oecd-ilibrary.org/science-and-technology/enhancing-the-digital-security-of-products_cd9f9ebc-en;jsessionid=CepkOlMMU3q3VuszF3M9uwED.ip-10-240-5-32

[20] Cyberspace Solarium Commission, ‘CSC Executive Summary.pdf’, Mar. 2020. Accessed: Mar. 01, 2021. [Online]. Available: https://drive.google.com/file/d/1c1UQI74Js6vk-fjUowI598NjwaHD1YtlY/view?usp=embed_facebook

[21] B. E. Humphreys, ‘Critical Infrastructure: Emerging Trends and Policy Considerations for Congress’, Congressional Research Service, R45809, Jul. 2019. [Online]. Available: https://www.everycrsreport.com/files/20190708_R45809_54416d7b2f43d41696e8e971832aea5fe96a9919.pdf

[22] House of Lords and House of Commons, ‘Cyber Security of the UK’s Critical National Infrastructure’, 2018. Accessed: Dec. 16, 2020. [Online]. Available: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf

[23] OECD, ‘Good Governance for Critical Infrastructure Resilience’, OECD Publishing, Paris, Text, 2019. Accessed: Mar. 19, 2021. [Online]. Available: https://www.oecd-ilibrary.org/governance/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en

[24] HM Government, ‘National Cyber Security Strategy 2016-2021’, 2016. Accessed: Dec. 16, 2020. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[25] NCSC, ‘2020 Annual Review’, NCSC, 2020. [Online]. Available: https://www.ncsc.gov.uk/annual-review/2020/index.html

[26] P. Muncaster, ‘Cybersecurity Skills Shortage Falls for First Time’, Infosecurity Magazine, Nov. 11, 2020. https://www.infosecurity-magazine.com:443/news/cybersecurity-skills-shortage-1/ (accessed May 18, 2021).

[27] P. M. Herder, I. Bouwmans, G. P. J. Dijkema, R. M. Stikkelman, and Margot P.C. Weijnen, ‘Designing infrastructures using a complex systems perspective’, Journal of Design Research, vol. 7, no. 1, pp. 17–34, Jan. 2008, doi: 10.1504/JDR.2008.018775.

[28] M. Ouyang, ‘Review on modeling and simulation of interdependent critical infrastructure systems’, Reliability Engineering & System Safety, vol. 121, pp. 43–60, Jan. 2014, doi: 10.1016/j.ress.2013.06.040.

[29] M. West, Developing High Quality Data Models. Elsevier, 2011. doi: 10.1016/C2009-0-30508-5.

[30] CDBB, ‘National Digital Twin Programme’, Centre for Digital Built Britain/University of Cambridge, Sep. 07, 2019. https://www.cdbb.cam.ac.uk/what-we-do/national-digital-twin-programme (accessed May 24, 2021).

[31] C. S. Wickramasinghe, D. L. Marino, K. Amarasinghe, and M. Manic, ‘Generalization of Deep Learning for Cyber-Physical System Security: A Survey’, in IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Oct. 2018, pp. 745–751. doi: 10.1109/IECON.2018.8591773.

[32] A. Y. A. Hammadi, C. Y. Yeun, and E. Damiani, ‘Novel EEG Risk Framework to Identify Insider Threats in National Critical Infrastructure Using Deep Learning Techniques’, in 2020 IEEE International Conference on Services Computing (SCC), Nov. 2020, pp. 469–471. doi: 10.1109/SCC49832.2020.00071.

[33] I. Kotenko, I. Saenko, A. Kushnerevich, and A. Branitskiy, ‘Attack Detection in IoT Critical Infrastructures: A Machine Learning and Big Data Processing Approach’, in 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), Feb. 2019, pp. 340–347. doi: 10.1109/EMPDP.2019.8671571.

[34] ENISA, ‘Artificial Intelligence Cybersecurity Challenges’, ENISA, Report/Study, Dec. 2020. Accessed: Mar. 19, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

[35] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, ‘Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios’, IEEE Access, vol. 8, pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[36] BT, ‘Protecting the UK’s Critical National Infrastructure’, London, 2017. [Online]. Available: https://business.bt.com/content/dam/bt/business/v2/PDF/Publicsector/BT_DSIC_white_paper.pdf

[37] M. Nouwens, C. Lons, N. Shehab, S. Malcomson, and A. Neill, ‘China’s Digital Silk Road: integration into national IT infrastructure and wider implications for Western defence industries’, International Institute for Strategic Studies, Feb. 2021. Accessed: Mar. 19, 2021. [Online]. Available: https://www.iiss.org/blogs/research-paper/2021/02/china-digital-silk-road-implications-for-defence-industry

[38] The Economist, ‘America’s war on Huawei nears its endgame’, The Economist, Jul. 16, 2020. Accessed: Mar. 19, 2021. [Online]. Available: https://www.economist.com/briefing/2020/07/16/americas-war-on-huawei-nears-its-endgame

[39] T. Madiega, ‘Digital sovereignty for Europe’, European Parliamentary Research Service, PE 651.992, Jul. 2020. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[40] C. Andrews, ‘Industry 4.0: challenges and opportunities’, Jul. 10, 2017. https://eandt.theiet.org/content/articles/2017/07/industry-4-challenges-and-opportunities/ (accessed May 18, 2021).

[41] J. Pan and Z. Yang, ‘Cybersecurity Challenges and Opportunities in the New “Edge Computing + IoT” World’, in Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, New York, NY, USA, Mar. 2018, pp. 29–32. doi: 10.1145/3180465.3180470.

[42] RISCS, ‘About Us | RISCS’. https://www.riscs.org.uk/about/ (accessed May 18, 2021).

[43] VeTSS, ‘Home’. https://vetss.org.uk/ (accessed May 18, 2021).

[44] RITICS, ‘About (Phase 2)’, RITICS. https://ritics.org/about/ (accessed May 18, 2021).

[45] RISE, ‘About RISE’, RISE UK Research Institute in Secure Hardware and Embedded Systems. https://www.ukrise.org/about/ (accessed May 18, 2021).

[46] CREST, ‘About’. https://crestresearch.ac.uk/about/ (accessed May 18, 2021).

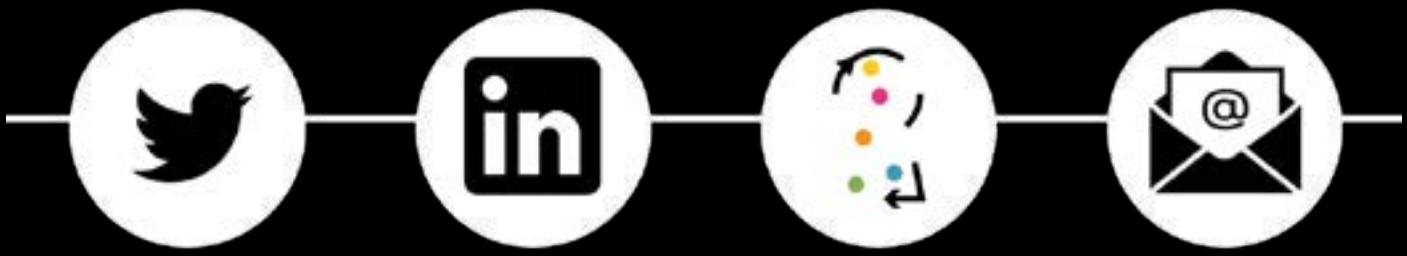
[47] C. Hankin et al., ‘Open Testbeds for CNI’, Research Institute in Trustworthy Industrial Control Systems (RITICS), 2018. [Online]. Available: http://ritics.org/wp-content/uploads/2018/07/Open-Testbeds_deliverable-final.pdf

[48] RITICS, ‘MUMBA’, RITICS. https://ritics.org/mumba/ (accessed Dec. 17, 2020).

[49] DAFNI, ‘About DAFNI’, Data & Analytics Facility for National Infrastructure - DAFNI. https://dafni.ac.uk/about-2/ (accessed Dec. 17, 2020).

[50] UKCRIC, ‘About UKCRIC’, UKCRIC. https://www.ukcric.com/about-ukcric/ (accessed Dec. 18, 2020).

[51] University of Bristol, ‘Facilities’. https://www.bristol.ac.uk/cdt/cyber-security/facilities/ (accessed Dec. 18, 2020).



TWITTER
@PETRASiot

LINKEDIN
linkedin.com/
school/petrasiot

WEBSITE
petras-iot.org

EMAIL
petras@ucl.ac.uk