Written evidence submitted by the NCC Group (CYB0008)

Introduction

NCC Group welcomes the opportunity to respond to the Committee's written call for evidence and to offer our expertise as a UK-headquartered global cyber security and software resilience business.

Through our threat intelligence, the research we undertake and the support we provide directly to the UK's critical national infrastructure (CNI), we are acutely aware of the cyber threat landscape, witnessing first-hand the real-world impact cyberattacks have on CNI and the ecosystems they support. **While the UK is, in many ways, at the forefront of cyber security (e.g. through our world-leading national technical authority, the NCSC), there are many fast-evolving challenges government, CNI operators and the supply chain must grapple with to build and maintain national cyber resilience**. Emerging technologies like AI have the potential to enable cyber attackers to mount ever more sophisticated campaigns against organisations, while the conflict in Ukraine has highlighted how CNI can be the target of coordinated cyber and physical attacks in a hybrid warfare setting.

In this response, we put forward practical considerations and recommendations for protecting CNI – and the citizens they serve – at scale, enabling them to thrive in the digital age. It is vital that the Government uses all its levers to prioritise and manage cyber threats, in partnership with the private sector, driven by a culture of information sharing and open dialogue.

Principally, we advocate for an approach that:

- **Keeps pace with technological and societal developments** – such as AI – by establishing flexibility, agility and periodic reviews and investing in long-term horizon scanning;
- **Expands the Cyber Assessment Framework (CAF) and GovAssure** to more effectively meet the challenges and threats faced by CNI, including by embedding 'Secure by Design' principles in these frameworks, addressing supply chain risks head on and, ultimately, ensuring they do not become just another 'tick box' exercise;
- **Mandates the adoption of realistic, intelligence-driven cyber security assurance testing**;
- **Establishes the evidence-base needed** to make informed decisions on cyber security policies, through the formation of an Office for National Cyber Statistics;
- **Reforms the UK's cyber laws, including the Computer Misuse Act 1990,** so that the UK's cyber defenders are able to do all they can to protect CNI from cyberattacks;
- **Looks beyond technical cyber risk** toward a wider understanding of what is needed to safeguard continuity of service against non-technical supply chain risks such as supplier failure, concentration risk and service deterioration;
- **Improves cyber literacy** so that all levels of society, age groups and professions, including senior public sector and CNI leaders, can make informed decisions about their personal and organisational cyber resilience;
- **Promotes close cooperation and collaboration with global allies**, particularly the 'Five Eyes'; and,

- **Trains and attracts a skilled cyber workforce** who can defend UK CNI.

Five years on since the Network and Information Systems (NIS) regulations introduced minimum cyber security requirements for CNI, we are pleased that the Committee is undertaking this timely review. We are keen to support the inquiry, sharing our expertise and insights from operating at the 'frontline' of cyber security. Below we set out our recommendations in more detail, responding directly to the inquiry's Terms of Reference. We would love the opportunity to explore these issues in more detail by providing oral evidence to the Committee.

About NCC Group

Driven by a purpose to create a more secure digital future, we are trusted by more than 14,000 clients worldwide to help protect their operations from ever-changing cyber threats. Our customers include operators of critical national infrastructure in a broad set of sectors from energy and financial services to communications and public sector, many of whom we have supported to comply with the NIS regulations. We work with organisations to identify and assess their security risks, remediate and manage vulnerabilities to improve their overall resilience and provide real-time detection and response. Our Threat Intelligence capability provides our customers with regular insights into the current threat landscape and the latest victims of cyber attacks, using software solutions to gather data on ransomware data leaks on the dark web in real time. We continually invest in research and development as an intrinsic part of our business model. Our research in areas like future telecoms security[1], artificial intelligence (AI)[2] and smart cities ensures we understand and can respond to the complex, rapidly evolving technological and threat environment.

Defining critical national infrastructure

As the Committee will be aware, the UK Government defines CNI as:

> *"Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:*
>
> *a) Major detrimental impact on the availability, integrity or delivery of essential services - including those services whose integrity, if compromised, could result in significant loss of life or casualties - taking into account significant economic or social impacts; and/or*
> *b) Significant impact on national security, national defence, or the functioning of the state."*

The Government has identified 13 national infrastructure sectors[3] which are subject to the NIS regulations that set minimum cyber resilience standards. It is with this definition and these sectors in mind that we base the majority of comments in our response. That said, against a backdrop of increasing digitalisation and drive toward net zero, the definition of

[1] 5G security – how to minimise the threats to a 5G network | NCC Group Research Blog | Making the world safer and more secure
[2] Whitepaper | Cyber Resilience in the Age of Artificial Intelligence - NCC Group
[3] Chemicals; Civil Nuclear; Communications; Defence; Emergency Services; Energy; Finance; Food; Government; Health; Space; Transport; Water.

what constitutes CNI is evolving. In the UK, the Government has set out plans to extend the NIS regulations to include managed service providers[4] and energy load controllers[5]. Some of the comments provided below respond to this evolution.

The types and sources of cyber threats to CNI most critical to the function of the UK digital economy

Sources

The majority of cyber attacks targeting CNI originate from either state and state-affiliated groups, or organised crime groups:

a) State and state-affiliated:

Principally, state and state-affiliated actors, with malign intent, continue to present a significant threat to CNI across all sectors. The type of threats posed by these actors vary, but, as set out by the National Cyber Security Centre (NCSC) in their 2022 Annual Review[6], include:

- **Cyber-enabled espionage** – unauthorised access or transfer of secret, classified or sensitive information to gain advantage over rivals.
- **Destructive cyber capabilities** – using tools such as wiper malware to damage IT systems or institutions, such as that seen with Distributed Denial of Service (DDoS) attacks (see more information on these types of attacks below).
- **Cyber-enabled theft** to further strategic advantage or domestic control, for example of Intellectual Property or personal data of citizens.
- **Hack and leak** – stealing and publishing sensitive or restricted information to embarrass states or institutions, or to undermine social cohesion.

Cyber threats should be seen in the wider context of nation state threats. The conflict in Ukraine has shown how cyber and kinetic attacks are increasingly interconnected in modern hybrid warfare[7]. As thousands of lines of complex code control new and evolving physical functions and systems, such as in smart cities, cyber security vulnerabilities can be (and are being[8]) exploited to effect change in the real-world. Whilst we have not seen the so-called 'cybergeddon' that some were expecting from the next big conflict on our globe, one thing is clear; cyber warfare has proven itself to be a critical element in a hybrid cyber-kinetic battlefield. In this conflict, we have seen the use of simple defacement and hacktivist activity, DDoS attacks and even the deployment of malware designed for sabotage and destruction of CNI.

b) Organised crime groups

While state and state-sponsored threats are a significant and evolving threat source, the threat from organised crime remains statistically higher. Indeed, 81% of the cyber incidents NCC Group responded to in 2022 were organised crime groups, while only 13% were nation-state or state-affiliated attacks (the remaining were either insiders or opportunists).

---

[4] See full definition in annex 1 here: Proposal for legislation to improve the UK's cyber resilience - GOV.UK (www.gov.uk)
[5] Organisations remotely controlling electrical load using communication networks.
[6] NCSC Annual Review 2022
[7] What the Russian Invasion Reveals About the Future of Cyber Warfare - Carnegie Endowment for International Peace
[8] Predatory Sparrow: Did hackers start this steel factory fire in Iran? - BBC News

Type

The majority of cyberattacks targeting CNI entail DDoS, ransomware and/or business email compromise:

a) Distributed denial of service (DDoS)

In terms of the types of cyberattacks we see undertaken on CNI, DDoS attacks – which entail the disruption of network services to make a machine or network resource unavailable – are prevalent. NCC Group's threat insights show that the UK experienced over 10,000 DDoS attacks in 2022[9], making it the third most targeted nation. The use of DDoS attacks combined with conventional military aggression in the Russia-Ukraine conflict has made it apparent that the cyber threat landscape has changed. Such attacks do not even need to bring down a service in its entirety to be impactful – a degradation of quality of service can be just as effective and more difficult to detect than a binary availability attack. These attacks are no longer seen as the purview of just amateur threat actors, but also as a significant tool of disruption utilised by some of the most prominent global threat actors and impactful campaigns of disruption.

b) Ransomware

NCC Group's insights show that, outside of the US, the UK is the most targeted country for ransomware attacks, which primarily (though not exclusively[10]) originate from cyber criminal groups. Indeed, ransomware has evolved significantly, becoming ever more sophisticated and underpinned by complex business models. In particular, we have observed the following developments:

- A significant increase in the sophisticated, targeted deployment of ransomware against selected high-value targets.
- As groups have sought to find a scalable business model, ransomware has evolved to Ransomware-as-a-Service (RaaS), which can be summarised by three key actors:
    - Initial access brokers obtain initial access to organisations' networks, selling this access to affiliates.
    - Ransomware operators, who own the malware source code, distribute it to affiliates after vetting their technical skills and their country of origin. Ransomware operators are also usually responsible for negotiating with victims.
    - Affiliates pay to use the malware developed by ransomware operators to target victims, agreeing on a service fee per collected ransom.

  As we see the development of the ransomware ecosystem, there are also other actors often involved in ransomware attacks, including data managers, accountants and negotiators. All this adds up to an increasingly complex system with tasks and functionality split across several actors in several geographies. It means that the ransomware attack vector has been opened up to a wider range of criminal actors where previously it was restricted to those with the requisite technical expertise. We also see criminal groups acting more and more like legitimate enterprises, implementing

[9] Annual Threat Monitor Annual Report 2022 - NCC Group

[10] North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector | CISA

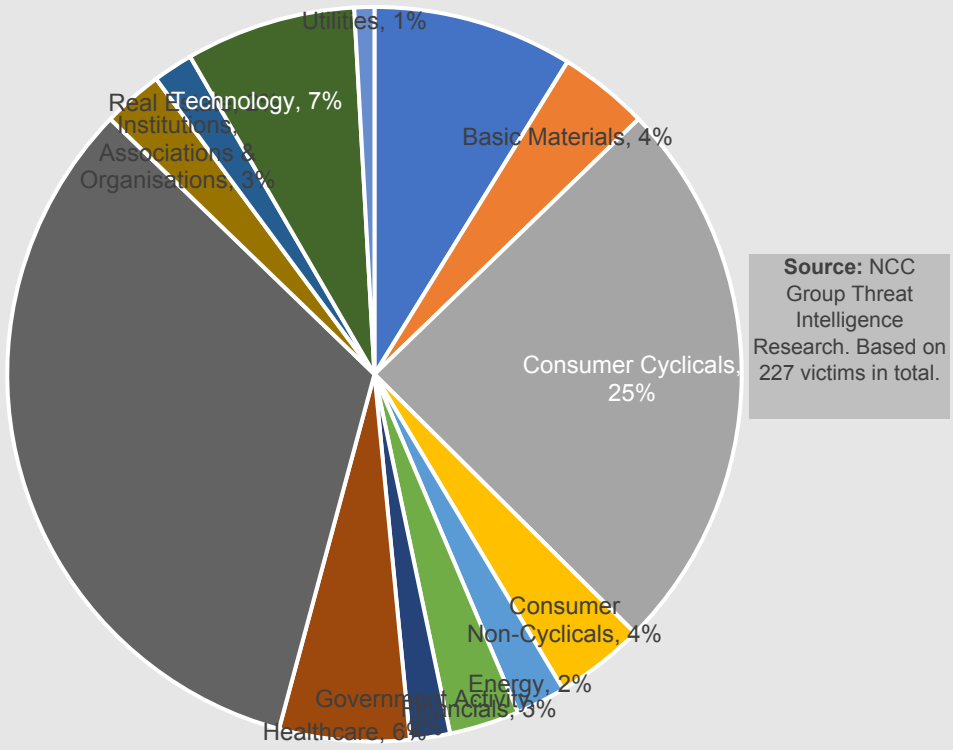
recruitment programmes and establishing HR functions (for example) with coordination around annual leave (as shown through the ContiLeaks[11]).

- We have also seen a rise in DDoS extortion attacks, whereby threat actors threaten to disrupt the normal traffic of a targeted system or network unless a ransom is paid. Unlike ransomware, actors performing DDoS extortion attacks do not need to access the company's systems or network. Instead, the targeted system or network is disrupted by overwhelming it, or its surrounding infrastructure, with a flood of internet traffic.
- In our experience, some of the more mature organisations within the financial services sector (such as larger retail banks) have seen a steady decline in successful ransomware attacks. As an early victim of cyberattacks, we believe that regulation has driven the widespread implementation of good cyber security practices across established financial firms. The sector provides an excellent case study of how well-formed regulation, combined with industry buy-in, can deliver good security outcomes, demonstrating the critical role that policymakers and regulators must play in building the UK's cyber resilience. However, it should be noted that the number of victims of double extortion ransom activity has remained constant (albeit low in volume), as our Threat Intelligence analysis has shown that less mature organisations, particularly insurers and investment managers, continue to be targeted successfully.

The extent to which sectors are resilient to cyberattacks will depend on a complex mix of incentives, governance, operational hygiene, corporate leadership and technical skills. Nevertheless, the below graph provides an overview of the number of ransomware victims across key sectors of the economy[12] in 2022, based on our analysis, and should provide the Committee with a sense of the most-targeted sectors in the UK. Of note, the industrials sector[13] was the most targeted sector by quite some margin, with consumer cyclicals[14] a notable second. We saw similar trends last year.

[11] Conti's blockchain plans: an ominous prospect | NCC Group Newsroom
[12] We categorise organisations based on The Refinitiv Business Classification: TRBC Sector Classification | Refinitiv
[13] The industrials sector includes: the manufacturing of industrial goods such as defence equipment, machinery and electrical components; construction and engineering; and, transport.
[14] The consumer cyclicals sector includes: the manufacturing of automobiles and consumer products; consumer services like hotels and leisure; media; and retailers.

Graph 1: UK-based ransomware victims by sector in 2022



c) Business email compromise

A business email compromise attack is a form of phishing attack[15] where a criminal attempts to trick a senior executive (or budget holder) into transferring funds or revealing sensitive information. While NCC Group responded to fewer business email compromise attacks than ransomware attacks in 2022[16], business email compromise still takes more money each year than ransomware when looking across the economy[17].

Attack vectors

There are several ways an attacker might gain a foothold in a victim's system, from a phishing email or exploiting an unpatched vulnerability, to exploiting a publicly facing application, such as a website. However, we would like to draw the Committee's attention to two attack vectors (or routes) which are of particular note among CNI sectors – legacy operational technology and the supply chain:

a) Legacy operational technology (OT)

[15] A technique involving fraudulent emails or messages designed to trick individuals into disclosing sensitive information or taking harmful actions, often by impersonating trusted entities or organisations. Phishing emails are also a major attack vector for ransomware attacks against organisations.
[16] Ransomware accounted for 40% of the incidents we responded to, while business email compromise accounted for 33%.
[17] 2021_IC3Report.pdf

A vector that cyber attackers are increasingly exploiting to target industrial sectors is via their legacy operational technology (OT) systems. The digital transformation of industries like energy and manufacturing is seeing OT assets, never designed with smart functionality in mind, overlayed with IT and hyper connectivity. Unlike IT, OT assets are usually designed to remain in operation for decades, and, as a result, OT systems are much more likely to include components that are 20 to 30 years old and/or use older software that is less secure and no longer supported. Integrating these legacy assets – which operators are eager to sweat and thus reluctant to replace – with modern security solutions can be very difficult. At the same time, the compromise of OT systems can be particularly impactful because they often interact with the "real world". Thousands of lines of complex code increasingly control physical systems like those seen in manufacturing plants or smart cities. This means that cyber security flaws can, and do[18], result in dangerous outcomes.

b) Supply chain

With the digitalisation of the economy, CNI organisations across all sectors are increasingly relying on third-party software and cloud providers for their critical functions and systems, opening up a new attack vector for malicious actors to exploit. While attacks mounted via an organisation's supply chain made up only 6% of the cyber incidents we responded to in 2022[19] , these types of attacks are increasing. Indeed, an NCC Group survey of 1,400 cyber security decision makers carried out last year found that cyber security attacks on company supply chains had increased by 51% in the prior six months[20].

The risks associated with the supply chain extend beyond cyber security to broader operational resilience too. Supplier failure or service deterioration – either as a result of a cyber attack or other factor such as insolvency – could have significant impacts on CNI organisations' ability to function, particularly where many are reliant on a handful of software and cloud providers, presenting a clear concentration risk. Some regulators, particularly in the financial services sector, are updating their guidelines to ensure CNI providers are managing these interrelated risks effectively. As we explore in more detail below, we are eager to see other regulators overseeing critical sectors follow suit.

It is worth noting that smaller organisations often act as important, or sometimes critical, suppliers to CNI operators. However, these organisations often lack the skills and budgets to implement proportionate cyber protections – leaving them exposed. Indeed, a recent UK Government survey[21] found that, due to rising costs and challenges with financial planning, smaller organisations were deprioritising cyber security measures. Smaller organisations can also be disproportionately affected when compared to their larger counterparts, with cyberattacks sometimes posing an existential threat. Another survey[22] found that 90% of European SMEs believed that cyber security issues would have serious negative impacts on their business within a week of the issues happening, with 57% saying they would most likely become bankrupt or go out of business. The conundrum of addressing the cyber security risk to small organisations - and the cyber threat their lack of resilience might pose to an economy as a whole - without unfairly burdening them with costly requirements remains a perennial challenge that has yet to be solved in a sustainable way. While we note

[18] Predatory Sparrow: Did hackers start this steel factory fire in Iran? - BBC News
[19] ncc-group-annual-threat-monitor-annual-report_final.pdf (nccgroup.com)
[20] 105503_ncc_insight_space_issue_6_no_dividers_v3.pdf (nccgroup.com)
[21] Cyber security breaches survey 2023 - GOV.UK (www.gov.uk)
[22] https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity

that this inquiry is looking primarily at CNI, given the role smaller organisations play in the wider ecosystem, we would ask that the Committee consider their cyber resilience too.

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

The UK Government is, in many regards, world-leading in its approach to tackling cyber security. The National Cyber Strategy has introduced genuinely pioneering initiatives, from expanding protection at scale, to acknowledging the role of offensive operations in national defence and putting cyber at the heart of the UK's foreign policy agenda. The Government Cyber Security Strategy 2022-2030, meanwhile, establishes an ambitious programme for public sector cyber resilience that is unrivalled globally in terms of its detail and clarity of timelines. Inevitably, changing government priorities has meant that the timings of some initiatives have shifted right; however, both strategies form a strong guiding light for building national cyber resilience that we are eager to see remain in place.

In terms of enhancing CNI cyber resilience, the principal method that the strategies promote is the adoption of the Cyber Assessment Framework (CAF) – an outcomes-based framework that provides a systematic approach to assessing and managing cyber risk – for NIS regulated sectors, and its public sector equivalent GovAssure. In our experience, both frameworks have been successful in standardising reporting around risk, helping Government to gain an accurate picture of the cyber threat landscape within specific sectors and enabling different organisations and role holders to speak the same language so that they are working together toward the same outcomes. That said, we believe that the CAF could be strengthened to more effectively meet the challenges and threats outlined above:

- **Embed 'Secure by Design' and 'Secure by Default':** The UK is a global champion for 'Secure by Design'[23] and 'Secure by Default'[24] principles that promote the integration of cyber security measures within a product, system or service from the start of – and throughout – its lifecycle. 'Secure by Design' and 'Secure by Default' represent a fundamental security concept for managing digital resilience in the modern age. They are particularly important for sectors like energy and manufacturing that are designing and implementing systems and infrastructure today that will be in place for up to 30 years. As we are currently experiencing with legacy systems in these industries, retrospectively securing a system years after it was designed is extremely difficult. It is much better to build security in from the outset. The current CAF does briefly mention 'Secure by Design'; however, we believe that these principles could be more explicitly embedded and promoted throughout the framework.
- **Avoid becoming just another 'tick box':** While the CAF is high-level and technology agnostic, it does still fundamentally remain a prescriptive list of requirements. Having such a reference model to design systems against can be useful; however, there are already a myriad of accepted standards out there that are widely used by CNI[25]. It is therefore important that Government considers how the CAF provides added value to CNI operators (beyond just copying and pasting

[23] Secure design principles - NCSC.GOV.UK
[24] Secure by Default - NCSC.GOV.UK
[25] These include: ISO 27001, US agency NIST's Cybersecurity Framework (CSF) and IEC 62443.

information from other frameworks into the CAF), while minimising the administrative burden of compliance.

- **Be clear about process:** While we do support the CAF's outcomes-based approach, it is important that the process for achieving that outcome is considered too.
- **Embed supply chain risks:** As outlined above, supply chain risks are a major concern for CNI, but there is very little in the CAF regarding how this should be managed. The Government, through the CAF, has standardised how it monitors cyber risk in the organisations it directly regulates. However, there are inconsistencies when it comes to how these various regulated organisations then manage the supply chain, which can result in insufficient minimum security levels and inefficiencies.
- **Clarity of responsibility:** Related to supply chain risks is the need for clearer delineation of roles between CNI operators and their suppliers. In our experience, responsibility for security is often pushed to other parties, particularly in complex supply chains. This is being partly addressed by extending the scope of the NIS regulations and putting additional requirements on critical providers. However, further guidance could be provided to CNI operators on building procurement regimes that embed 'Secure by Design' from the outset.

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

The UK's National Cyber Security Centre (NCSC), is, in our experience, the envy of the world, providing excellent technical advice for businesses and organisations looking to improve their cyber resilience and promoting information sharing and mutual learning within and across CNI sectors through formalised information exchanges. Recognising that cyber skills are in great demand, NCSC also works extremely well with the private sector to deliver a genuinely whole-of-society response, through initiatives like Industry100. We ask that Government continue to ensure that NCSC is well-resourced so that it can continue with its important, world-leading endeavours.

Within central Government, cyber security in CNI is overseen by several departments and Ministers. The Cabinet Office has principal responsibility for the implementation of the Government's cyber strategies, the Department for Science, Innovation and Technology (DSIT) is responsible for CNI cyber policy and legislation, the Home Office oversees cybercrime and several other Government departments and regulators act as the 'Competent Authorities'[26] for the implementation of the NIS regulations within their sector. With cyber security being such a cross-cutting issue, this division of responsibility is inevitable and necessary for ensuring policy decisions reflect the realities of those they will impact. There are some excellent examples of good government policy and initiatives that have enhanced UK CNI's cyber resilience in recent years, including DSIT's 'Secure by Design' principles, the CHERI project that is developing ground-breaking secure computer chips and the initial implementation of the NIS directive. That said, the split responsibility between and within government Departments can sometimes mean that policy is developed in siloes and it is not always clear where responsibility for certain issues sits. In addition, as

[26] 'Competent authority' is the term used in NIS for a regulatory body. There are multiple competent authorities responsible for different sectors covered by NIS. A list of other competent authorities is published in Schedule 1 of NIS: The Network and Information Systems Regulations 2018 (legislation.gov.uk)

highlighted in a recent Public Accounts Committee report[27], a lack of digital skills and understanding of cyber security across senior leaders in central Government can mean that necessary investments in cyber resilience are deprioritised.

The result has been an often-complex policy and investment landscape that is difficult for businesses to navigate and contribute to. To overcome this issue, we recommend that further effort is made to develop new (and cultivate existing) cross-departmental working groups on core cyber issues, ensuring lessons learned are shared across sectors and minimising overlapping policy development. The Government should also invest in upskilling senior public sector leaders, so that they can make informed decisions about cyber resilience within their field of responsibility.

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

As the Committee point to, public-private partnerships are a critical part of the UK's "whole of society" approach to enhancing cyber resilience. In particular, the UK's cyber industry is working closely with law enforcement, the public sector, academia and other private firms to ensure the UK remains confident, capable and resilient in this fast-moving digital world. Vulnerability researchers, for example, identify security vulnerabilities in products, software and services, and work with manufacturers and vendors to fix them before they can be exploited by malicious actors for nefarious purposes. Meanwhile, threat intelligence researchers detect cyberattacks and gain insight into attackers and victims, often in real time. Researchers then work with and pass on this important information to law enforcement and intelligence agencies, enabling them to defend UK CNI against rising cybercrime and geo-political threat actors.

However, the current legal framework, specifically the Computer Misuse Act 1990, is holding back a large proportion of cyber security researchers from doing all they can to protect the UK. This is because the Act, which was written over 30 years ago, blankly prohibits all forms of unauthorised access to computer material, irrespective of intent or motive. NCC Group has long been a strong advocate for reform of the Act which, we believe, if done correctly, will greatly strengthen researchers' ability to fight the scourge of cybercrime, supporting national cyber resilience, driving growth and helping to cement the UK as a global cyber power. Indeed, in his report to Government on the 'Pro-Innovation Regulation of Technologies'[28], former Chief Scientific Adviser Sir Patrick Vallance recommended "amending the Computer Misuse Act 1990 to include a statutory public interest defence that would provide stronger legal protections for cyber security researchers and professionals and would have a catalytic effect on innovation in a sector with considerable growth potential." We were pleased to see the Chancellor commit to implementing Sir Patrick's recommendations in the Spring Budget. The Home Office has since launched a multi-stakeholder process to consider whether defences for legitimate cyber security activity should be embedded in the Act. We are expecting an update on progress before the end of the year. In the meantime, we would be grateful for anything the Committee could do to make the case for a 21st century Act that reflects modern cyber security practices.

---

[27] Whitehall staffing cuts add to digital skills shortages and risk increased costs - Committees - UK Parliament
[28] Pro-innovation_Regulation_of_Technologies_Review_-_Digital_Technologies_report.pdf (publishing.service.gov.uk)

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

Principally, the Government must set measurable targets for CNI operators, and ensure these are clearly communicated, within good time, to the right stakeholders. Clarity of the North Star that the CNI ecosystem is working toward will be key.

In terms of enhancing CNI cyber resilience, there is no silver bullet solution. CNI resilience is a complex, ever-evolving problem that requires a complex, ever-evolving response. We do, nevertheless, believe that there are a number of measures that should be prioritised as part of the nation's response:

An Office for National Cyber Statistics

A foundational building block will be a reliable, extensive dataset on the cyber threats facing the UK (and our allies). While data on cyber incidents across CNI and the supply chain is available to sectoral regulators, there is currently no centrally coordinated effort to bring these metrics together to build a full picture of the cyber threat landscape. A fuller centralised data set would allow the Government to prioritise threats, allocate resources to policy efforts, and measure the success of those efforts. As US National Cyber Director Chris Inglis recently commented[29] when speaking about analogous considerations in the US, "to properly address risk, we have to first understand it, we have to understand where it's concentrated, where it cascades, what causes it, and more importantly to then discover how to address it." Similarly, NATO conducts its analysis by putting its adversaries – what they are doing, what their intent is and what their capabilities are – first when planning for operations.

We propose establishing an Office for National Cyber Statistics that anonymises, collates and disseminates incident data from existing sources (for example, Action Fraud incident response data, public sector threat information which – in future – is set to be automated and enhanced right across Government, and incidents reported by CNI under the NIS regulations) and new sources (for example, working with the cyber threat intelligence and incident response community to more systematically share incident response information).

Regulating for CNI – today and tomorrow

We are pleased to see the Government's recognition that the NIS regulatory framework must be flexible and able to adapt to the inevitable evolution of what constitutes the UK's CNI. To that end, we welcome confirmed plans to legislate to enable Government to bring new sectors within scope of the NIS regulations – to include, in the first instance, managed service providers and energy load controllers. It is crucial that there are no delays in bringing forward these reforms and that a Bill is prioritised for the forthcoming King's Speech. Failure to legislate would leave a core part of the UK's CNI exposed, where others globally are already moving forward with new laws to ensure all relevant entities are appropriately and proportionately regulated.

---

[29] National cyber director backs new Bureau of Cyber Statistics - FCW

We do also expect evolving sectors, such as the nation's network of electric vehicle chargers, to be critical in the not too distant future. While it may not be appropriate to designate these sectors as CNI today, the Government should consider what proportionate security and resilience measures these sectors should be taking now to ensure they are not vulnerable to cyberattacks in future. As outlined above, sectors like energy and transport will be developing and integrating infrastructure today, that will be in place for years, if not decades, to come. It is important, therefore, that these assets are built with security in mind and that we do not wait until these sectors are seen as critical before securing them. Improved horizon scanning would help Government to understand what the future of CNI looks like and prepare for it.

Adoption of intelligence-led testing across CNI

We believe there is a need for more widespread adoption of realistic, intelligence-driven cyber security assurance testing across CNI sectors, alongside the continued adoption of the CAF. The value of such testing has been clearly demonstrated by the CBEST scheme[30] led by the Bank of England for the financial sector, and adopted by the telecoms, civil nuclear and government sectors. The schemes allow the participants, regulators, NCSC and the Government to understand the cyber risks and resilience issues and respond to the needs of the sector. They are intelligence-led, so the ethical attack teams replicate the tactics, techniques and procedures of known threat actors. Organisations learn what and how attacks could have an impact, assess their ability to detect and respond and measure the return of their investment and training in improving their cyber resilience. Meanwhile, regulators gain important insight as to the actual real-world resilience and risk to their sector, which could be fed back – on an anonymised basis – to the centrally coordinated Office for National Cyber Statistics we proposed above, to help build a (more authoritative) nationwide picture of the threat.

Tackling the wider risk landscape

As outlined above, the increasing reliance on third-party providers across large parts of the economy, including CNI, not only presents cyber security risks but also wider risks to operational continuity such as supplier failure (e.g. bankruptcy), service deterioration, concentration risk, political risks and transfer of ownership. Therefore, building a truly resilient CNI also requires the Government to look beyond technical cyber risk toward a wider understanding of what is needed to safeguard continuity of service against these non-technical risks. This concept of operational resilience is being embedded in regulators' frameworks globally, particularly in the financial services sector. For example, the UK Prudential Regulation Authority (PRA)[31] names concentration risk, service deterioration, supplier failure and political risks as risks that need to be mitigated through firms' business continuity plans, requires scenario testing of these risks and mandates that end users build demonstrably successful stressed exit plans[32]. It also recommends practical resilience measures such as escrow solutions that can help to mitigate against supply chain failure. Similar guidelines have been put in place by the PRA's global counterparts[33], as well as

---

[30] CBEST Threat Intelligence-Led Assessments | Bank of England

[31] SS2/21 'Outsourcing and third party risk management' (bankofengland.co.uk)

[32] A stressed exit is when the contract is ended due to the failure or insolvency of the service provider, and therefore is more unexpected than a non-stressed exit, which could be due to commercial, performance or strategic reasons.

[33] Including, but not limited to: Europe (Digital finance: Council adopts Digital Operational Resilience Act - Consilium (europa.eu)); Singapore (TRM-Guidelines-18-January-2021.pdf (mas.gov.sg)); Australia (APRA consults on new prudential standard to strengthen operational resilience | APRA); Switzerland (FINMA publishes Circular "Operational risks and resilience – banks" | FINMA); Canada (Operational resilience key definitions (osfi-bsif.gc.ca)); the US (SEC.gov | SEC Division

embedded in key international standards like ISO27001[34] and the US Cybersecurity and Infrastructure Security Agency (CISA) whose guidance on ransomware[35] states that, in being prepared for a ransomware incident, organisations should ensure the availability of the source code that underpins critical systems through backups or escrow agreements.

A national programme of 'cyber literacy'

Use of regulatory levers aside, there is much more that could be done to improve understanding of cyber security concepts across organisations of all sizes and at all levels of seniority, so that decision-makers can make informed decisions about their cyber resilience proportionate to the risks they face. We need a step change to demystify cyber and embed awareness and incentives into everyday conversations, to make it an integral part of our national psyche. At the heart of this should be the concept of 'pervasive cyber literacy' - a basic level of cyber competence across all levels of society, age groups and professions to allow everyone to use technology securely. This could involve:

- The deployment of behavioural insights experts to shift user behaviour so that device security updates and other basic measures are further embedded in the nation's psyche as standard practice.
- A renewed focus on the people element of cyber security, developing human cyber risk skills and their interactions with technology or human factors.
- Commissioning 'Cyber Beebies', keeping with the concept of CBeebies to "help pre-schoolers learn while they play fun games, watch clips, sing songs and make things", to start cyber education and awareness in the earliest years.
- Including cyber competence, covering safe and secure online behaviours, privacy, and use of technology alongside broader computing lessons, as a mandatory part of the school curriculum, which should be reviewed and tested with an industry advisory board on a regular basis to ensure it keeps pace with technological developments and industry requirements. Teachers must also be regularly supported to understand new developments and how they should be reflected in the school curriculum.

As well as establishing a base-level of digital and cyber literacy across society, we also need to train and attract a skilled cyber workforce who can defend UK CNI. However, there remains a significant skills shortage, and much more needs to be done to encourage talent into the profession, particularly those from diverse and underrepresented backgrounds, as well those with crosscutting skills (e.g. those which bridge cyber security and related disciplines like engineering and safety). Initiatives should include:

- Efforts to make cyber security attractive for all, committing explicitly to measure trends in the proportion of candidates coming into the cyber profession from non-traditional backgrounds or at different and varying points in their adult lives.
- The creation of a national institute for secondary and integrated further education, targeted at exceptionally gifted cyber security students, to build up a cadre of excellence, and a deployable elite in multi-disciplinary cyber domain matters. The Government could also consider introducing an assessment for all secondary school children to assess their suitability for a career in cyber security.

---

of Examinations Announces 2023 Priorities).
[34] ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements
[35] Ransomware Guide | CISA

Global cooperation

When it comes to tackling cyber threats, no country is an island. The criminal landscape is complex, involves many actors and the complicit involvement of nation states, with cyberattacks very rarely originating from the UK alone. In addition, even if the UK was impervious to cyberattacks, overseas suppliers – many of whom are critical to the functioning of the UK economy and CNI – may not be. Close international cooperation is therefore critical and should be front and centre of UK policymakers' minds when developing the UK's approach. Specifically, we recommend that the Government:

- Utilises existing successful partnerships, including the 'Five Eyes' alliance and the US-led International Counter Ransomware Initiative (CRI), strengthening global cooperation and coordination against criminal gangs;
- Invests time in developing practical outcomes with other governments, that go deeper than high-level principles;
- Ensures that civil society and industry - who will play a central role in delivering governments' objectives - are involved in discussions from the outset; and,
- Works with partners to disrupt financial flows of, and disincentivise, ransomware actors, including through greater regulation of crypto exchanges, use of individual indictments and red notices, and enhanced coordination across borders.

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'

As outlined above, we believe that 'Secure by Design' is a fundamental security concept for managing digital resilience in the modern age. It is particularly important for sectors like energy and manufacturing that are designing and implementing systems today that will be in place for up to 30 years. With that in mind, we urge policymakers to more explicitly embed the concept in the CAF GovAssure frameworks.

Emerging technology (AI)

AI has the potential to greatly improve productivity, automate tasks and provide access to computer-generated capabilities which might previously have been out of reach. In the world of cyber security, it is being used by cyber defenders to analyse large data sets at scale, support threat intelligence and mimic the behaviours of cyber attackers, so that organisations can understand and prepare for potential attacks. It is also likely that generative AI will, in future, support the development of secure software code; however, such technology is currently unreliable and still requires expert oversight and other traditional controls to ensure accuracy. Indeed, NCC Group research[36] has explored large language model (LLM) secure code generation, finding that while the model that was assessed was impressive in its ability to generate usable code, human expert review identified a number of oversights which could lead to security flaws.

[36] Machine Learning 103: Exploring LLM Code Generation | NCC Group Research Blog | Making the world safer and more secure

Where AI is being used by cyber defenders for benevolent purposes, it can also be exploited by cyber attackers for malevolent purposes. AI is effectively lowering the barrier of entry into cybercrime, making it easier for cyber attackers to successfully target victims and widening the availability of voice cloning, deep fakes and social engineering bots. We are likely to see this manifest in the following ways:

- **Higher volume of cyberattacks:** Greater automation will like mean higher numbers of attacks.
- **Generation of malware:** There are signs of cybercriminals looking to use LLMs to generate malicious code for use in cyberattacks.
- **Improved success rate of social engineering and phishing attacks:**
    - The gradual improvements in the speed and quality of deepfakes now mean that they are a feasible approach to social engineering by mimicking the voice and even the face of trusted people in telephone or video calls.
    - Phishing emails are often poorly written and formatted, so much so that it is commonplace for cyber security awareness training to advise to be wary of emails with poor spelling and grammar. LLMs present an opportunity to phishing email writers to improve the spelling, grammar and tone of the text in their emails. This threat has been recognised by the developers of LLM-based chatbots and guardrails are deployed to prevent the explicit generation of phishing text, but it is very difficult to detect the intent behind a message if the prompt does not specifically ask for text to be used in phishing but instead phrases it as a marketing or security message.
    - Spear-phishing - which entails a targeted phishing attempt tailored to an individual or organisation - can also be improved using generative chatbots, enabling attackers to quickly generate targeted messaging for a wide variety of potential targets.

While developers typically implement controls to prevent malicious or unethical outputs from AI systems, NCC Group research has shown that it's possible to circumvent these protections to exfiltrate and weaponise LLMs' training data[2]. Meanwhile, our Global Threat Intelligence practice has observed evidence of cybercriminals collaborating on the dark web to find ways to bypass the controls in ChatGPT. They are also increasingly seeing advertisements for an LLM, WormGPT, developed without guardrails that can be used for malicious purposes[37].

While the evidence of the malicious use of AI by cyber attackers is, at present, largely anecdotal[38], and we currently assess the increase in cyber risk as a direct result of AI to (today) be small to moderate, even a moderate increase in risk, against the backdrop of the wider fast-evolving cyber threat landscape, is noteworthy and requires action. It is therefore important that the Government build these considerations into its regulatory framework for CNI cyber resilience.

More broadly, to keep pace with any technological and societal developments – whether that be AI or other impactful changes such as the recent shift to working from home, reliance on cloud or the rapid adoption of smart home devices – flexibility, agility and periodic reviews need to be built into the Government's approach. This should be supported by coordinated and improved horizon-scanning. Indeed, across government, the private sector and

[37] Whitepaper | Cyber Resilience in the Age of Artificial Intelligence - NCC Group
[38] We are yet to see these techniques come through in the cyberattacks we are responding to on a daily basis.

academia, there is already a myriad of horizon scanning and forecasting activity and initiatives which aim to stay on top of the increasingly complex risk landscape. There are also a number of government bodies and advisers whose remit involves considering future risks and opportunities, including the Regulatory Horizons Council, departmental Chief Scientific Advisers, Scientific Advisory Councils and departmental expert advisory groups and councils such as DSIT's College of Experts. The Government should review what assessments are already being undertaken, and how this analysis could be better coordinated and drawn upon, so that horizon-scanning work results in actionable information for building national cyber resilience.

6 November 2023