Cyber resilience of the UK's critical national infrastructure - Nominet submission to the Call for Evidence

08 November 2023

Submission from Nominet, the .UK Internet Domain Name Registry

This is the Nominet submission to the Science, Innovation and Technology Select Committee's call for evidence on cyber resilience of the UK's Critical National Infrastructure (CNI). Our submission covers the strengths and weaknesses of the UK Government's National Cyber Strategy 2022 and Government Cyber Security Strategy 2022-2030 (the Strategies) in relation to CNI for the digital economy. Further information on Nominet is provided in the Appendix to explain why our expert opinion is relevant to the Committee.

Internet infrastructure:

The focus of the Strategies is on systems and data *connected to the Internet*. This means the *infrastructure of the Internet* itself is not covered to the same extent with regards to CNI. This is possibly due to the fact the Strategies define Cyber Security as '*the protection of internet-connected systems … from unauthorised access, harm or misuse*', which inadvertently implies Internet infrastructure is somehow peripheral to the Strategies.

What's missing: The Strategies would be significantly strengthened by additional clarification on the role of Internet infrastructure to the cyber security of CNI.

UK leadership in development of digital standards that affect the Internet:

The Strategies rightly point to the need to uphold an open and interoperable Internet and highlight the importance government sees in participation in international fora that influence digital standards underpinning the Internet. Such standards underpin the cyber security of all the UK's digital CNI. Powerful actors (including nation states and global corporations) now '*defend their political and economic interests through the formulation of technical standards and protocols*' (quote from the EU Parliamentary Research Service report on the splinternet 2022). This reality is publicly acknowledged by government in a number of national strategies, including the Integrated Review, Digital Strategy and International Technology Strategy, and by the UK's recent endorsement of the Declaration for the Future of the Internet.

What's missing: The Strategies would be strengthened by explaining how the UK will develop the additional capacity required to protect the multistakeholder governance of Internet technical standards from interference by powerful actors.

Amplifying multistakeholder international cyber capacity building:

The Strategies provide a strong argument for the need for effective *multilateral* organisations and partnerships to build international cyber capacity. They highlight working with the United Nations, Five Eyes, NATO, G7, European Union, Commonwealth, OECD, Global Forum on Cyber Expertise (GFCE), ASEAN Forum, African Union and the World Bank.

What's missing: Government should explore whether there is a need to establish an effective multistakeholder international institution bringing together nations, public and private sector organisations and civil society groups with similar democratic values that can develop international cyber capacity.

Greater alignment across the regulatory and compliance landscape:

There are a swathe of different UK and international digital regulations and standards beyond those specific to cyber security that UK companies are required to comply with, or in some cases voluntarily follow, to support their value chains. For example, although it is not something the UK has to transpose into domestic legislation, the EU's NIS 2 Directive will impact UK value chains and therefore UK businesses will have to put in place processes to ensure they do not adversely diverge from NIS 2 in a way that would add additional burden for their business partners.

Many CNI operators, such as energy suppliers and transport network operators, are large corporations. Other organisations that are key to supporting CNI, such as Nominet and other internet operators like LINX, are much smaller and should be seen as essentially SMEs. While it is important that the principle of cyber security should be recognised everywhere, it is also important that the application of deterrents, standards and certifications should be proportionate to the scale of the organisations concerned.

What's missing: The Strategies would be strengthened by recognising the complexity of the entirety of the regulatory and compliance landscape and the need for government to take a holistic view of how to support UK companies. They would also be strengthened by clarifying the need for proportionality with regards the scale of organisations supporting CNI.

Tensions between freedom of expression, privacy, safety and security:

The National Cyber Strategy 2022 references that it is complementary to the Online Safety Bill (OSB). There is a fundamental tension between imposing safeguarding, privacy and freedom of expression requirements on technology through the OSB whilst the Strategies expect the same technology to have stringent cyber security capabilities.

What's missing: The Strategy would be strengthened by explaining the democratic process by which inevitable policy compromises between privacy, freedom of expression, safety and security will be developed if both the OSB and the Strategies are to be effective in practice. This is necessary to ensure future technologies can be developed in a way that is compliant with all the various regulatory frameworks and still provide adequate cyber protection of CNI.

Secure by Design Principles:

The Strategies rightly emphasise the importance of industry adopting Secure by Design Principles. The US Cybersecurity and Infrastructure Security Agency's report from April 2023 on principles and approaches for Secure by Design software, which is co-signed by twenty national security agencies including NCSC, states '*too many manufacturers place the burden of security on the customer rather than investing in comprehensive application hardening*'. That report states Secure by Design principles are not being adopted at the necessary scale, yet the concept of secure by design has existed for the past twenty years.

What's missing: If we are to try and get software manufacturers to make Secure by Design the default, we need to be clear on how that translates to product development, deployment and maintenance, prove the business value of it to organisations (particularly SMEs) and explore barriers to uptake in adopting its principles.

Reflections on Nominet's experience as an operator of an essential service

Nominet is an 'Operator of Essential Services' under the Network and Information Systems (NIS) Regulations 2018, and is therefore required to take appropriate and proportionate technical and organizational measures to manage risks posed to the security of the network and information systems on which our essential service relies. We welcome the UK taking an outcomes-focused, principles-based approach to regulation, including through the NCSC's Cyber Assessment Framework, which outlines the acceptable security levels for organisations who fall under NIS requirements. We also value the way in which our regulator, OFCOM, works with us to enforce requirements in a collaborative and iterative way, which strengthens regulator capability while ensuring our business has the strongest internal security and information management policies possible.

Appendix: Further information about Nominet

The appendix provides information about Nominet to establish that we have the depth and breadth of expertise to provide authoritative evidence that is relevant to the committee.

Principle based

- Nominet follows the overarching principle that the internet should be developed, governed, operated and used for the benefit of society.

Crucial to the UK's Digital Infrastructure

- Nominet manages the top level country code '.uk' internet domain name registry. Domain names are commonly referred to as web-addresses. For example, 'bbc.co.uk' and 'gov.uk'. Domain name registries are used by web-browsers, mobile phone apps and computer operating systems to find the correct internet protocol (IP) addresses needed to connect to online content, data centres and cloud-computing services.
- The registry handles over 200 billion queries and updates each month to cope with the ever-increasing demand from organisations as they digitalise their core business. Over three million UK businesses depend on the registry to function online.
- We are designated by government as an operator of an essential service within scope of the Network and Information Systems (NIS) Act 2018. As such we play a crucial role in supporting the UK's digital infrastructure.

Protecting the Public Sector from Malware, Ransomware and Phishing Attacks

- Nominet implements the Protective DNS service (PDNS) on behalf of the National Cyber Security Centre (NCSC) as part of the UK's Active Cyber Defence Programme. It protects over a thousand public sector organisations from accessing internet domain names connected with malware or phishing attacks. Nominet successfully rolled out PDNS to protect the vaccine supply chain during the Covid-19 pandemic. In 2022 the PDNS system handled over 86 billion queries per month and blocked over five million attempts to access internet domain names associated with ransomware.

Shaping How the Internet is Used to Improve Lives

- Nominet has committed £65m over a five year period to initiatives that use technology to change lives through our Social Impact programme.
- Four flagship social impact projects will bring about lasting societal change. They are ClickStart – a new digital social mobility scheme to help over 25k people, developed with the Institute of Coding; equipping

every primary school in the UK with BBC Micro:bits to teach children essential computing skills; supporting the UK Safer Internet Centre to counter child online harms; and bridging the digital divide by significantly amplifying our work with the Good Things Foundation.

Supporting the UK's International Leadership of Internet Governance

- Nominet supports the UK's participation in internet governance through multistakeholder forums such as the UN's Internet Governance Forum (IGF), the European Dialogue on Internet Governance (EuroDIG), and the Internet Corporation for Assigned Names and Numbers (ICANN). This helps to keep the internet governed by democratic values and not undermined by authoritarianism.

Tackling Illegal Activity on the Web

- Nominet runs a world leading voluntary domain name suspension programme working with UK law enforcement agencies to disrupt online criminal activity. Just over two thousand domain names identified as conducting criminal activity were suspended in 2022 as a result of notifications from thirteen UK law enforcement agencies.
- Nominet's anti-phishing initiative, Domain Watch, further increases the safety of the '.uk' namespace. Using machine learning, it flags potentially malicious domains at the point of registration to Nominet's in-house compliance team for them to determine if they are for legitimate use.