House of Lords
House of Commons

Joint Committee on the National Security Strategy

Cyber Security of the UK's Critical National Infrastructure

Third Report of Session 2017–19

Report, together with formal minutes relating to the report

Ordered by the House of Lords to be printed 12 November 2018

Ordered by the House of Commons to be printed 12 November 2018

HL Paper 222
HC 1708
Published on 19 November 2018
by authority of the House of Lords
and House of Commons

The Joint Committee on the National Security Strategy

The Joint Committee on the National Security Strategy is appointed by the House of Lords and the House of Commons to consider the National Security Strategy.

Current membership

House of Lords

Lord Brennan *(Labour)*

Lord Campbell of Pittenweem (*Liberal Democrat*)

Lord Hamilton of Epsom (*Conservative*)

Lord Harris of Haringey (*Labour*)

Baroness Healy of Primrose Hill (*Labour*)

Baroness Henig (*Labour*)

Lord King of Bridgwater (*Conservative*)

Baroness Lane-Fox of Soho (*Crossbench*)

Lord Powell of Bayswater (*Crossbench*)

Lord Trimble (*Conservative*)

House of Commons

Margaret Beckett MP (*Labour, Derby South*) (Chair)

Yvette Cooper MP (*Labour, Normanton, Pontefract and Castleford*)

James Gray MP (*Conservative, North Wiltshire*)

Mr Dominic Grieve MP (*Conservative, Beaconsfield*)

Dan Jarvis MP (*Labour, Barnsley Central*)

Dr Julian Lewis MP *(Conservative, New Forest East)*

Angus Brendan MacNeil MP (*Scottish National Party, Na h-Eileanan an Iar*)

Robert Neill MP (*Conservative, Bromley and Chislehurst*)

Rachel Reeves MP (*Labour, Leeds West*)

Tom Tugendhat MP (*Conservative, Tonbridge and Malling*)

Stephen Twigg MP (*Labour (Co-op), Liverpool, West Derby*)

Theresa Villiers MP (*Conservative, Chipping Barnet*)

Powers

The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place within the United Kingdom, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chairman.

Publications

The Reports of the Committee are published by Order of both Houses. All publications of the Committee are on the Internet at www.parliament.uk/jcnss.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are Simon Fiander (Commons Clerk), Matthew Smith (Lords Clerk), Ashlee Godwin (Commons Senior Specialist), Georgina Hutton (Acting Commons Committee Specialist), Matthew Chappell (Commons Committee Assistant), Breda Twomey (Lords Committee Assistant) and Estelle Currie (Press Officer).

Contacts

All correspondence should be addressed to the Commons Clerk of the Joint Committee on the National Security Strategy, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 8586; the Committee's email address is jcnss@parliament.uk.

Contents

Summary

The head of the National Cyber Security Centre (NCSC) has said that a major cyber attack on the United Kingdom is a matter of 'when, not if'. The UK's critical national infrastructure (CNI) is a natural target for such an attack because of its importance to daily life and the economy. However, public opinion as yet has only a limited appreciation of what could befall us as a result of cyber attacks, which present as credible, potentially devastating and immediate a threat as any other that we face.

The Government has explicitly acknowledged that it must do more to improve the cyber resilience of our critical national infrastructure, irrespective of whether it is owned or operated in the public or private sector. While we applaud the aspiration, it appears the Government is not delivering on it with a meaningful sense of purpose or urgency. Its efforts so far certainly fail to do justice to its own assessment that major cyber attacks on the UK and interests are a top-tier threat to national security.

The threat to the UK and its critical national infrastructure is both growing and evolving. States such as Russia are branching out from cyber-enabled espionage and theft of intellectual property to preparing for disruptive attacks, such as those which affected Ukraine's energy grid in 2015 and 2016. The 2017 WannaCry attack, which affected the NHS, also demonstrated that cyber attacks need not target critical national infrastructure deliberately to have significant consequences. In addition, some organised crime groups are becoming as capable as states, thereby increasing the number and range of potential attackers.

The objective must therefore be to make it as difficult and as costly as possible to succeed in attacking the UK's critical national infrastructure—and to continue raising the bar as new threats emerge.

In the two years since the current National Cyber Security Strategy was published, the Government has taken some important steps. These include establishing a national technical authority on cyber security—the NCSC—and introduced more robust regulation for some, but not all, CNI sectors. That tightened regulatory regime was not the Government's own initiative but instead flows from our acceptance of EU-wide regulations. Moreover, though a useful step forward, it will not be enough to achieve the required leap forward across the thirteen CNI sectors.

The Government must do much more to change the culture of CNI operators and their extended supply chains, ensuring that these issues are understood and addressed at board level and embedding the view that cyber risk is another business risk that must be proactively managed. This is also a lesson for the Government itself: cyber risk must be properly managed at the highest levels.

We also reported in July on the importance of addressing the shortage in specialist skills and deep expertise and urged the Government to prioritise delivering its cyber security skills strategy.

Getting ahead and staying ahead of the threat in these ways will require strong and sustained leadership. The NCSC is undoubtedly fulfilling its remit in providing technical leadership on cyber resilience, although we are concerned that expectations of the NCSC are outstripping the resources put at its disposal by the Government.

More significantly, identifiable political leadership is lacking. There is little evidence to suggest a 'controlling mind' at the centre of Government, driving change consistently across the many departments and CNI sectors involved. Unless this is addressed, the Government's efforts will likely remain long on aspiration and short on delivery. We therefore urge the Government to appoint a single Cabinet Office Minister who is charged with delivering improved cyber resilience across the UK's critical national infrastructure.

1 Introduction

1. Since 2010 the Government has categorised major cyber attacks on the UK and its interests as a top-tier threat to national security. This means that such an attack is highly likely and/or would also have a high impact.[1] The impact of technology, and especially of cyber threats, was identified as one of the four "particular challenges … likely to drive UK security priorities for the coming decade" in the 2015 National Security Strategy and Strategic Defence and Security Review 2015 (2015 NSS & SDSR).[2] Its importance was reaffirmed by the Government's National Security Capability Review in March 2018.[3]

2. The past year has seen cyber attacks on the health, telecommunications, energy and government sectors in the UK.[4] And although the UK has yet to suffer the most severe form of cyber attack—which the Government defines as an attack leading to the sustained loss of essential services, severe economic or social consequences, or a loss of life[5]—the head of the National Cyber Security Centre (NCSC), Ciaran Martin, has said this is a matter of 'when', not 'if'.[6] The May 2017 WannaCry attack, which affected NHS services for several days, should serve as a stark warning of the implications of such an attack for national security.

3. There are also important implications for the UK's future prosperity—one of the three strategic objectives of the 2015 NSS & SDSR.[7] The effects of a major cyber attack on a just-in-time economy should not be underestimated.[8] Furthermore, the UK's ability to reap many of the economic benefits of future technology such as internet-connected devices (the 'Internet of Things'), automation and robotics will depend on robust cyber security—and, as importantly, public confidence in that cyber security.

4. Given the Government's emphasis on cyber threats in the 2015 NSS & SDSR, as well as the string of high-profile cyber attacks in 2016 and 2017, we decided to launch an inquiry into the cyber security of critical national infrastructure (CNI) as our first inquiry of the 2017 Parliament.[9] The Government has identified thirteen national infrastructure sectors

[1] HM Government, *Fact Sheet 2: National Security Risk Assessment*, October 2010, accessed 1 November 2018; HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, Cm 9161, November 2015, Annex A

[2] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, Cm 9161, November 2015, para 3.3

[3] The National Security Capability Review identified two additional 'particular challenges', making the impact of technology, including cyber threats, one of six. HM Government, *National Security Capability Review*, March 2018, p. 5, para 2

[4] Q54 [David Lidington MP]

[5] National Cyber Security Centre (NCSC), "Annual Review 2018", October 2018, p. 23

[6] "Major cyber-attack on UK a matter of 'when, not if' – security chief", The Guardian, 23 January 2018

[7] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, Cm 9161, November 2015

[8] The International Institute for Strategic Studies (CNI0017) para 4

[9] Our predecessor Committee launched an inquiry entitled "Cyber Security: UK National Security in a Digital World" in January 2017. The Committee took written evidence and held one oral evidence session before the June 2017 general election was called and Parliament was dissolved.

that are essential to the functioning of daily life: chemicals; civil nuclear; communications; defence; emergency services; energy; finance; food; government; health; space; transport; and water.[10] We set out to examine:

- the types and sources of cyber threats to CNI in the UK;
- the extent to which the Government's definition of 'critical national infrastructure' is still valid in an interconnected economy;
- learning points drawn from the 2011 Cyber Security Strategy and the fitness for purpose of the 2016 Cyber Security Strategy in relation to CNI;
- the effectiveness of the strategic lead provided by the National Security Council, Government departments and agencies, and the NCSC, and the coherence of cross-government activity;
- the effectiveness of the Government's relationships with private-sector operators and regulators in protecting CNI from cyber attack;
- the balance of responsibilities between the Government and private-sector operators in protecting CNI against cyber attack;
- the consistency of approach in the UK to legislation, regulation and standards governing each CNI sector and cyber security;
- the availability of skills and expertise to the relevant Government departments and agencies, to regulators, and to private-sector operators of CNI; and
- the extent to which the UK's approach to the cyber security of CNI draws on or represents international best practice.

We published these terms of reference and a call for evidence for our inquiry in December 2017.[11] Reflecting the weight of the evidence we received, our inquiry has focused primarily on issues relating to continuity of critical services, rather than the cyber-enabled theft of personal data or threats to democratic processes (which have been addressed by other Committees),[12] although we recognise their significance. We also acknowledge the Government's work to develop 'cyber weapons' under the National Offensive Cyber Programme but this was not an area covered by our inquiry.[13]

[10] According to the Government's Centre for the Protection of National Infrastructure (CPNI), not everything within a national infrastructure sector is judged to be "critical". The Government's official definition of CNI is: "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."
See CPNI, "Critical National Infrastructure", accessed 28 June 2018

[11] The inquiry terms of reference and call for evidence can be found on the Joint Committee on the National Security Strategy website.

[12] House of Commons Digital, Culture, Media and Sport Committee, Fifth Report of Session 2017–19, *Disinformation and 'fake news': Interim Report*, HC 363; House of Commons Science and Technology Committee, Fourth Report of Session 2017–19, *Algorithms in decision-making*, HC 351; House of Lords European Union Committee, Third Report of Session 2017–19, *Brexit: the EU data protection package*, HL Paper 7; House of Commons Exiting the European Union Committee, Seventh Report of Session 2017–19, *The progress of the UK's negotiations on EU withdrawal: Data*, HC 1317

[13] HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, para 6.5; *"UK becomes first state to admit to offensive cyber attack capability"*, Financial Times, 29 September 2013; Intelligence and Security Committee of Parliament, *Annual Report 2016–2017*, HC 655, Section 6; HM Government, *Budget 2018*, HC 1629, para 5.26 and Table 2.1

5. In February 2018 we held a private roundtable discussion on the cyber security of CNI, facilitated by techUK and attended by representatives of its member organisations.[14] We took oral evidence in public from UK CNI operators (from representatives of the energy, transport and health sectors) as well as CNI-sector regulators and a trade body (representatives of the financial services, energy and communications sectors and the water sector, respectively). Our third evidence session focused on the shortage of essential cyber security skills.[15] In June 2018 we took oral evidence from the Chancellor of the Duchy of Lancaster, Rt Hon David Lidington MP—the Cabinet Office Minister responsible for the delivery of the National Cyber Security Strategy 2016–2021 (2016 NCSS)—and Ciaran Martin, Chief Executive Officer of the NCSC. These two witnesses also gave us a private briefing after their evidence session.

6. This Report is the second of our inquiry. In July we published *Cyber Security Skills and the UK's Critical National Infrastructure*, in which we concluded that

> there are not enough people in the UK who both possess [the required] specialisms and are also willing and able to work in the CNI sector.[16]

Immediate and longer-term solutions must be found to this challenge. We are not reassured in this regard by the Government's response to our Report on cyber security skills. Although positive in tone, it does not commit the Government to sufficient concrete action in the short term, with most of the initiatives referred to seemingly set to bear fruit towards the end of the next decade.[17] Without a concerted, wide-ranging and creative effort to close the skills gap, this shortage in specialist skills and deep technical expertise will severely hinder the Government and the private sector in improving the UK's CNI resilience to cyber threats at the pace required. The findings set out in this Report on the cyber security of CNI should be seen in that light.

7. We are grateful to all those who have provided written and oral evidence to our inquiry and to that of our predecessor Committee. We also thank our Specialist Adviser for the inquiry, Ewan Lawson, and our standing Specialist Advisers, Professor Malcolm Chalmers, Professor Michael Clarke and Professor Sir Hew Strachan, for their input.[18]

[14] These organisations were Arqiva, CGI, Palo Alto Networks and Splunk.

[15] Many of those CNI operators and regulators that provided evidence said that a shortage of skills is one of the greatest challenges they face in relation to cyber security. Q20 [Rob Shaw]; Q27; Q29; Q39 [Rob Crook, Dr Alastair MacWillson]; techUK (CNI0015) para 4; BT Group (CNI0018) para 8.1; Nokia (CNI0022) para 7.1

[16] Joint Committee on the National Security Strategy, Second Report of 2017–19, *Cyber Security Skills and the UK's Critical National Infrastructure*, HL Paper 172, HC 706, para 15

[17] Joint Committee on the National Security Strategy, Second Special Report of 2017–19, *Cyber Security Skills and the UK's Critical National infrastructure: Government Response to the Committee's Second Report of Session 2017–19*, HL Paper 198, HC 1658

[18] Ewan Lawson declared the following interests relating to this inquiry on 26 February 2018: Senior Research Fellow, Royal United Services Institute; Senior Teaching Fellow, Centre for International Studies and Diplomacy, SOAS, University of London; member of and unpaid adviser to Scottish National Party. Professor Malcolm Chalmers declared the following interests relating to this inquiry on 18 December 2017: Deputy Director-General, Royal United Services Institute. Professor Michael Clarke and Professor Sir Hew Strachan declared no interests relating to this inquiry. The full declarations of interests by Ewan Lawson, Professor Malcolm Chalmers, Professor Michael Clarke and Professor Sir Hew Strachan are available in the Committee's Formal Minutes 2017–19.

2 Protecting CNI against cyber attack: a 'wicked' problem

Dynamic threats

8. In the two years since the Government's National Cyber Security Strategy 2016–2021 (the 2016 NCSS) was launched, more than 1,000 cyber attacks have required the involvement of the NCSC—an average of ten a week.[19] Although most of these will not have affected the UK's CNI, these figures do include the May 2017 WannaCry attack, which affected NHS services, as well as attacks on the UK and Scottish Parliaments in June and August 2017, and on the energy and telecommunications sectors.[20] The past year has also seen the Government start to make joint or coordinated announcements with other countries that publicly attribute major attacks to other states. The most noteworthy of these in relation to CNI was the Technical Alert released jointly with the United States in April 2018, which disclosed Russia's "sustained presence in UK and US internet infrastructure".[21]

9. In their evidence, David Lidington and Ciaran Martin told us that the cyber threat is both growing and changing in nature as it grows.[22] This is most evident in relation to the perpetrators behind cyber attacks on the UK's CNI. The NCSC's latest Annual Review reports that state actors continue to "constitute the most acute and direct cyber threat to our national security", having perpetrated the majority of the incidents dealt with by the NCSC since it was established in October 2016.[23] Russia has inevitably garnered many of the media headlines about cyber attacks in recent months—especially as the Government has now publicly attributed many major attacks to the Russian state, including the June 2017 NotPetya and the October 2017 BadRabbit attacks, both of which appeared to target Ukraine but had a much wider impact.[24] However, the NCSC's latest Annual Review acknowledges that "There is much, much more to the cyber security threat to the UK than just Russia".[25] For example, the WannaCry attack was attributed by the UK and US Governments to the North Korean state-sponsored Lazarus hacking group. The media also widely reported that Iran was responsible for the June 2017 attack on Parliament, while China's alleged theft of corporate secrets and intellectual property (IP) has prompted the US Government to set up a taskforce to counter cyber-enabled economic espionage by China.[26] These incidents also demonstrate the range of motivations behind state-conducted cyber attacks.

[19] NCSC, "Annual Review 2018", October 2018, p. 10; NCSC, "Annual Review 2017", October 2017

[20] See, for example, *"Russian cyber attacks have targeted UK energy, communication and media networks, says top security chief"*, The Independent, 15 November 2017

[21] Q59 [Ciaran Martin]

[22] Q54; NCSC, "Annual Review 2018", October 2018, p. 22

[23] 'State actors' include groups that are "directed, sponsored or tolerated" by the Governments of hostile states. NCSC, "Annual Review 2018", October 2018, p. 10

[24] *"UK exposes Russian cyber attacks"*, NCSC press release, 4 October 2018

[25] NCSC, "Annual Review 2018", October 2018, p. 10

[26] NCSC, "Annual Review 2018", October 2018, p. 10; *"Iran blamed for parliament cyber-attack"*, BBC News, 14 October 2017; *"Iran attacks 9,000 email accounts in Parliament"*, The Times, 14 October 2017; *"Iran to blame for cyber-attack on MPs' emails—British intelligence"*, The Guardian, 14 October 2017; Federal Bureau of Investigation, *"Combating Economic Espionage"*, 1 November 2018, accessed 5 November 2018; *"In Chinese Spy Ops, Something Old, Something New"*, ForeignPolicy.com, 5 November 2018

10. However, while states continue to be the dominant actors behind cyber threats to the UK, we heard that their behaviour and apparent motivations are changing. The Cabinet Office notes that states are "starting to explore offensive cyber capabilities to damage, disrupt or destroy the systems or networks of their adversaries", whereas previous campaigns had tended to focus on espionage and IP theft.[27] Ciaran Martin singled out Russia as being particularly problematic in this regard, citing "a consistent rise in [its] appetite for attack on critical sectors" and its 'prepositioning' for future disruptive attacks.[28] Referring to the joint Technical Alert released with the United States in April, he explained that Russia has established

> a foothold [in the UK's internet infrastructure], an intrusion that you can use for ongoing espionage purposes or can develop as the potential for a hostile, disruptive and destructive act in the future.[29]

He added that Russia has also begun to diversify its targets, for example to include "softer-power democratic institutions". North Korea has similarly changed its approach, moving from "political retaliation attacks"—by attacking Sony Pictures in 2014, for instance—to "the theft of money",[30] through ransomware attacks such as WannaCry and reportedly stealing more than $81 million from the central bank of Bangladesh in February 2016 via the SWIFT payments system.[31]

11. It is also clear that states are no longer the only actors with the ability and resources to attack CNI, which generally benefits from more advanced defences than other parts of the economy. Ciaran Martin told us that

> We have seen an evolution of cybercrime, where some of the most sophisticated attackers [such as organised crime groups] are now operating at almost nation-state level.[32]

NCC Group, a UK-based cyber security and risk mitigation services company, agreed, adding that where organised crime groups work in association with—or with the acquiescence of—states such as Russia, the lines between them are becoming increasingly blurred.[33] [34] Ciaran Martin also raised "the risk of proliferation", whereby state and non-state actors can buy more sophisticated cyber tools and techniques on what has become a "highly developed market".[35] The result is that "It is now easier and cheaper than ever before for those who want to do us harm to access the tools, exploits and services they

[27] Cabinet Office, National Security Secretariat (CNI0013) para 2

[28] Q54 [Ciaran Martin]; NCSC, "Annual Review 2018", October 2018, p. 10

[29] Q59 [Ciaran Martin]

[30] Q54 [Ciaran Martin]

[31] In September, the US Justice Department formally charged an alleged North Korean spy for helping to perpetrate the 2014 cyber attack on Sony Pictures, in apparent protest at the impending release of the film *The Interview*, the 2016 cyber attack on the Bangladesh Bank, and the 2017 WannaCry ransomware attack. *"North Korean 'hacker' charged over cyber-attacks against NHS"*, The Guardian, 6 September 2018

[32] Q54 [Ciaran Martin], BT Group reported that the majority of the cyber attacks it experiences are conducted by organised crime groups. BT Group (CNI0018) para 2.2

[33] NCC Group (CNI0002) para 2.1.1. See also Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, 2017) *"Why the Russian Government Turns a Blind Eye to Cybercriminals"*, Slate, 2 February 2018; *"Licensed to hack: the rise of the cyber privateer"*, Financial Times, 16 March 2017

[34] The Cabinet Office told us that: "A range of other cyber actors also present a potential threat to UK CNI, including hacktivists and terrorists, although we judge these threats to be low." Cabinet Office, National Security Secretariat (CNI0013) para 5

[35] Q54 [Ciaran Martin]

need to launch attacks."[36] Furthermore, as the 2017 WannaCry and NotPetya attacks demonstrated, cyber attacks do not need to target the UK's CNI specifically in order to affect it. As Ciaran Martin stated, "in 2017 we learned to watch out for the reckless as well as the deliberate."[37]

Complex challenges

12. We heard that there are particular challenges involved in protecting CNI against cyber attack. The first of these is the reliance of CNI not only on IT systems, but also on operational technology (OT) systems, such as electricity substations, transportation control rooms and their associated industrial control systems.[38] These bespoke and often legacy industrial control systems, which were not designed with cyber security in mind, are now increasingly networked and connected to the internet to enable more efficient control and real-time monitoring. This has the effect of creating new vulnerabilities and potentially exposing the systems to cyber attack.[39] The complexities of OT systems also make it difficult to patch vulnerabilities once they have been identified. The Cambridge Centre for Risk Studies explained that CNI operators must consider the implications for safety, the equipment's warranty, the asset's physical location, the need to minimise downtime and the usability of connected systems before doing so.[40]

13. Ciaran Martin described the move towards next-generation OT systems built with resilience in mind as the "great strategic opportunity" of the next decade, although he was also keen to stress that 'secure by design' does not mean that devices and systems are "impervious" to cyber attack.[41] [42] Nevertheless, the question still remains as to how legacy OT systems can be protected against cyber attack in the meantime, as new vulnerabilities emerge and threats continue to evolve.[43]

14. The second key challenge is that with some key exceptions—such as health, defence and government—the majority of CNI is privately owned and is therefore beyond the Government's direct control.[44] This raises difficult questions for the Government about how far to intervene in the operations of private companies to ensure that national security interests are prioritised and about what types of intervention would be most effective (see

[36] NCSC, "Annual Review 2018", October 2018, p. 6

[37] Q54 [Ciaran Martin]

[38] OT generally refers to systems that control physical devices while IT generally refers to information storage and integrity—with IT systems including traditional PCs, company servers and networks, cloud storage, smartphones and tablets. Cambridge Centre for Risk Studies (CNI0025) para 1

[39] NCC Group (CNI0002) para 2.1.2; Nettitude (CNI0003) para 9; Cambridge Centre for Risk Studies (CNI0025) para 2

[40] Cambridge Centre for Risk Studies (CNI0025) paras 3–5. It also highlights the "strict procedure" required in the UK for any modification of a medical device, including the installation of a cyber security patch. Cambridge Centre for Risk Studies (CNI0025) paras 6–9
The Financial Conduct Authority adds a further consideration: the size of the network in question. It states that "implementing patches (evaluating, prioritising and deploying) in a global estate of over one million endpoints for a critical vulnerability is a significant task and so fundamental cyber resilience capabilities remain a significant concern". Financial Conduct Authority (CNI0033) para 6.3

[41] Q63 [Ciaran Martin]. The NCSC's 2018 Annual Review describes its work in designing secure next-generation vehicles, a new sustainable energy grid and the UK's new spaceports. NCSC, "Annual Review 2018", October 2018, p. 30

[42] Systems can be designed to perform narrowly defined actions and only accept instructions from verified sources, and networks can be designed to minimise the impact of any single failure. *Cyber Security of UK National Infrastructure*, POSTnote No. 554, May 2017

[43] UK Computing Research Committee, UKCRC (CNI0005) para 1

[44] University of Oxford cyber security researcher Jamie Collier cites one estimate, dating from 2011, suggesting that as much as 80% of UK CNI is in private ownership. Jamie Collier (CNI0006) para 2

Chapter 4). In addition, many CNI operators are utility providers whose funding streams are pre-agreed, often by regulators, and limited by price controls.[45] Without a more flexible approach to price controls, the question often asked in relation to cyber security—'how much is enough?'[46]—can become particularly acute for these CNI operators.[47]

Resilience, not security

15. Independent cyber security researcher Pete Cooper observed that protecting CNI against cyber attack presents a 'wicked' problem, in that it is "both novel and complex, which can slow decision making, collaboration and innovation". He also stressed that when it comes to CNI, the UK cannot afford to wait and learn through experience.[48] The 2017 WannaCry attack had a relatively limited impact, in view of the widespread exposure of systems to the vulnerability targeted,[49] but it demonstrated the potential consequences of not being sufficiently proactive in managing cyber risk to CNI operations.

16. However, as Sean Kanuck, Director for Cyber, Space and Future Conflict at the International Institute for Strategic Studies (IISS), told us, it is "impossible to predict [changes in threat, the identification of vulnerabilities and new methods of attack] far enough in advance to institutionally prepare for them all". It is therefore "essential to … adopt a strategy that stresses resilience of networks in lieu of 'security' per se."[50] This means preparing for and adapting to changing circumstances, with the focus on making it more difficult for the attacker rather than trying to attain a certain level of security. It also means minimising the impact of attacks—some of which will inevitably succeed—by having fully rehearsed plans in place to respond to and recover from them as quickly as possible.[51] [52]

17. David Lidington told us that even the most advanced sectors in terms of cyber risk management—such as the financial services sector—"can never be complacent … because there will be organisations right now trying to work out how to get round the security measures that big financial institutions have put in place."[53] Steve Unger, Chief Technology Officer at the communications regulator Ofcom, told us

> Together with government we need to find a way of upping our game in this area in what is ultimately an arms race, but doing so in a way that is still deliverable and not kidding ourselves that there is a silver bullet in any of this.[54]

[45] For example, Ofgem's Jonathan Brearley and Water UK's Paul Smith told us that investment in cyber security by operators in the energy and water sectors is limited by price controls set years in advance by the respective regulators during price reviews. Q31

[46] Pete Cooper (CNI0019) para 9

[47] Q18 [Phil Sheppard]

[48] Pete Cooper (CNI0019) para 24

[49] Cisco (CNI0016) para 1.2

[50] The International Institute for Strategic Studies (CNI0017) para 4. Rowland Johnson, Chief Executive of cyber security company Nettitude, reports that in 2017 an average of 50 new vulnerabilities were disclosed every day to MITRE, a cyber security organisation tracking vulnerabilities. Nettitude (CNI0003) para 17

[51] Department for Homeland Security, "What is Security and Resilience?", accessed 1 November 2018

[52] Q8 [Rob Shaw]; Q63 [Ciaran Martin]

[53] Q63 [David Lidington MP]

[54] Q38 [Steve Unger]

Open source software provider Red Hat Inc. stated that the practical implications of this is that frameworks for managing cyber risk must be "iterative" in nature, taking account of new techniques and technologies as they become available.[55] Pete Cooper agreed, concluding that

> there is no 'end state' for cyber security … the new norm must be continual defensive innovation and resilience in the face of determined and creative adversaries.[56]

As such, while a long-term strategy is necessary to set the direction of travel for the Government and CNI operators, regular review of and updates to implementation plans would allow the Government to be more agile in responding to this rapidly changing environment. It would also enable the Government and operators to take better advantage of technological innovation, which is essential given that our adversaries are highly innovative and also invest heavily in their capabilities.[57]

18. **The cyber threat to the UK's CNI is growing. It is also evolving: hostile states are becoming more aggressive in their behaviour, with some states—especially Russia—starting to explore ways of disrupting CNI, in addition to conducting espionage and theft of intellectual property. Furthermore, while states still represent the most acute and direct cyber threat, non-state actors such as organised crime groups are developing increasingly sophisticated capabilities.**

19. **Fast-changing threats and the rapid emergence of new vulnerabilities make it impossible to secure CNI networks and systems completely. Continually updated plans for improving CNI defences and reducing the potential impact of attacks must therefore be the 'new normal' if the Government and operators are to be agile in responding to this changing environment and in taking advantage of constant technological innovation. Building the resilience of CNI to cyber attacks in this way will make it harder for an attacker to achieve their objective—whoever that attacker may be, whatever their motive and however they choose to attack.**

[55] Red Hat Inc (CNI0021) para 30

[56] Pete Cooper (CNI0019) Executive Summary

[57] Manchester Metropolitan University (CNI0001) para 4.2; UK Computing Research Committee, UKCRC (CNI0005) para 5; Glasswall Solutions Limited (CNI0007) paras 4.2, 4.5, 4.7, 4.9; Cabinet Office, National Security Secretariat (CNI0013) paras 12, 16, 64; BT Group (CNI0018) para 6.5; Corero (CNI0023) para 9; CyLon (CNI0032) para 1

3 The National Cyber Security Strategy 2016–2021 and CNI

20. The Government's approach to cyber security, writ large, is framed by the 2016 NCSS, which was published in November 2016.[58] It explicitly recognises that the "market based approach" to cyber security under the earlier 2011 strategy had not achieved "the scale and pace of change required to stay ahead of the fast moving threat".[59] As such, it acknowledges the need for the Government to "intervene more directly", "by bringing its influence and resources to bear to address cyber threats".[60] It states:

> The UK Government, in partnership with the Devolved Administrations of Scotland, Wales and Northern Ireland, will work with the private and public sectors to ensure that individuals, businesses and organisations adopt the behaviours required to stay safe on the Internet. We will have measures in place to intervene (where necessary and within the scope of our powers) to drive improvements that are in the national interest, particularly in relation to the cyber security of our critical national infrastructure.[61]

21. Many of those who submitted written evidence to our inquiry and that of our predecessor Committee welcomed the step change in Government approach in the 2016 NCSS, with some describing the strategy—and the activity it underpins—as world-leading.[62] This appears to be borne out by the notable level of international interest in the UK's approach to cyber security, which is reported in the NCSC's 2018 Annual Review; the NCSC's CEO Ciaran Martin refers directly to other countries' "admiration" for it.[63] However, there appears to be little beyond anecdotal evidence that the UK is at the forefront of international efforts on cyber security. As we observed in relation to cyber security skills,[64] a more methodical, rigorous comparison with allies and adversaries alike would be beneficial to the UK in benchmarking and continually improving its own approach.[65]

[58] HM Government, *National Cyber Security Strategy 2016–2021*, November 2016. Commitments relating to protecting CNI are set out in Section 5.4.

[59] HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, paras 1.3, 2.7

[60] HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, para 2.7

[61] HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, para 1.7

[62] techUK (CNI0015), paras 3, 4.1; Nokia (CNI0022) para 5.1; Aerospace, Defence, Security and Space (CNI0020) paras 1.10–1.11; Palo Alto (CNI0011) para 5; UK Computing Research Committee, UKCRC (CNI0005) para 8; Glasswall Solutions Limited (CNI0007) para 4.1; The International Institute for Strategic Studies (CNI0017) paras 4, 8–9; Altran UK (CNI0008) para 6; Chatham House (CNI0012) para 5.4; Red Hat Inc (CNI0021) para 13; ISACA (CNI0010) para 2.2; BT (CYB0025) paras 4.1–4.2; PA Consulting (CYB0009) para 6. By contrast, Manchester Metropolitan University stated that the 2016 NCSS "should be looking to make the United Kingdom a world-leader in cybersecurity rather than proclaiming it has already achieved this." Manchester Metropolitan University (CNI0001) para 4.1

[63] NCSC, "Annual Review 2018", October 2018, pp. 11, 17

[64] Joint Committee on the National Security Strategy, Second Report of 2017–19, *Cyber Security Skills and the UK's Critical National Infrastructure*, HL Paper 172, HC 706, para 13

[65] Dr Martyn Thomas (CNI0004) para 9.1; Glasswall Solutions Limited (CNI0007) paras 9.1–9.3; The International Institute for Strategic Studies (CNI0017) para 8; Red Hat Inc (CNI0021) para 16; Corero (CNI0023) paras 12–13 The Government states that it "frequently draws upon the approaches and expertise of other countries in its cyber security work", citing various visits to US institutions as examples. Cabinet Office, National Security Secretariat (CNI0013) para 51

Defining 'critical' national infrastructure

22. The 2016 NCSS does not address what the Government's priorities are in protecting the UK's CNI from cyber attack. Indeed, the strategy adds "priority sectors" to the established list of thirteen sectors, citing "other companies and organisations, beyond the CNI, that require a greater level of support."[66] This is in contrast to the approach taken in the US Government's September 2018 National Cyber Strategy, which identifies seven "key areas" from within its list of sixteen 'critical infrastructure sectors'.[67]

23. The principal purpose of defining 'critical' infrastructure should be to enable the Government and industry to prioritise their efforts, focusing their attention on those assets whose failure or impairment would have the greatest impact on the UK's national security and its economy. However, with every CNI sector now "systemically connected",[68] more government and business processes being automated,[69] internet-connected devices proliferating under the Internet of Things,[70] and even entire cities designed to be 'smart',[71] it is more difficult than ever to determine where truly 'critical' infrastructure ends and where the 'wider economy' begins.

24. BT Group observed that "the Government's definition of Critical National Infrastructure (CNI) is too wide … and therefore no longer helpful in terms of identifying the key parts of UK infrastructure that need enhanced protection."[72] ISACA, a professional association for IT governance, suggested the Government adopt a tiered approach to CNI sectors, with some tiers treated as 'firsts among equals'.[73] The NCSC reports that it has been working with lead Government departments to map "critical systems" across CNI sectors to better understand their "interconnectedness" and, therefore, improve their resilience.[74] This should, as the NCSC Annual Review notes, help establish priorities for Government intervention based on an "overarching view" of CNI. Such work is highly important, given the potential impact and risk of "cascading" failures between interconnected sectors, which we heard are not yet well understood.[75]

[66] This "premium group" includes the UK's "most successful companies", with an emphasis on research and development and intellectual property, "data holders" such as charities, which hold data on "vulnerable citizens"; "high-threat targets", such as media organisations, with an emphasis on preventing damage to the UK's reputation and public confidence in the Government; digital service providers that underpin the economy; and organisations with influence over the entire economy, such as insurers, investors, regulators and professional advisors. HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, para 5.4.1

[67] These areas are: national security; energy and power; banking and finance; health and safety; communications; information technology; and transportation. White House, *National Cyber Strategy*, September 2018, pp. 8–9. The full list of sixteen 'critical infrastructure sectors' is available at Department for Homeland Security, "Critical Infrastructure Sectors", accessed 30 October 2018

[68] Nettitude (CNI0003) paras 9–10; Pete Cooper (CNI0019) para 1; Nokia (CNI0022) para 3.2

[69] This might include, for example, electoral registration processes and the Universal Credit system. Q56 [Ciaran Martin]; NCC Group (CNI0002) para 2.2.2.1

[70] The International Institute for Strategic Studies (CNI0017) para 5; Nettitude (CNI0003) para 9

[71] Q56 [Ciaran Martin]; Nokia (CNI0022) para 3.3; Department for International Trade, "Speech: The UK's leadership in smart cities", 28 March 2018, accessed 30 October 2018

[72] BT Group (CNI0018) para 3.1

[73] ISACA (CNI0010) para 1.4

[74] NCSC, Annual Review 2018, 16 October 2018, p. 30.

[75] Pete Cooper (CNI0019) paras 1–2; The International Institute for Strategic Studies (CNI0017) paras 4–5; Nokia (CNI0022) paras 3.1–3.2

25. The 2016 NCSS also does not differentiate between the varying complexity of the CNI sectors in terms of the number and type of organisations that fall within the threshold for 'critical' infrastructure.[76] In some sectors, such as defence, government and water, a relatively small number of organisations are responsible for 'critical' assets. In these sectors there are only a few institutions for the Government to work with and, in the case of defence and government, it has a high degree of control or influence over them. By contrast, 'critical' assets in finance, food and transport are more varied, with key organisations covering only a small part of the sectors involved. In such sectors, governmental action must necessarily be more indirect, with fewer bodies closely connected to the Government and with corporate activity inherently more market-led and less institutionalised. This variation in complexity across the CNI spectrum affects how sectors engage with cyber security and act to improve resilience. It will consequently have an important bearing on how the Government should prioritise its efforts and assess the results.

26. **'Critical' national infrastructure is, by definition, a priority for the Government and industry. However, as the economy becomes more interconnected, it is increasingly difficult to determine which elements are truly critical. The 2016 National Cyber Security Strategy provides few clues as to how the Government is managing this issue or how it is prioritising its efforts between CNI sectors. It also fails to acknowledge the varying complexity of the CNI sectors and the bearing this should have on the Government's approach. Asserting that the UK is at the forefront of international efforts on cyber security is not sufficient.**

27. ***The next National Cyber Security Strategy, due for publication in 2021 should be informed by a mapping of the key interdependencies between CNI sectors—and therefore of national-level cyber risk to CNI—which the Government should complete as soon as possible and keep under continual review. The priorities identified in the next Strategy should also take account of the CNI sectors' respective maturity in terms of cyber resilience and the varying levels of Government influence over operators in each sector.***

Setting and delivering strategic objectives, and measuring progress

28. Most of those who submitted written evidence were positive about the ambition encapsulated in the 2016 NCSS. However, Dr Martyn Thomas of Gresham College criticised it for lacking a "credible roadmap" with specified "key milestones", describing it as "a set of tactics rather than a strategy".[77] This appears to us to be a fair description of the section in the Strategy on CNI,[78] which lacks:

[76] Although the Government defines thirteen broad infrastructure sectors as 'critical', not all operators within these sectors are designated as CNI. Each sector has its own threshold for determining what is, and is not, a critical asset and therefore should be treated as such. For the energy sector, for example, it is any energy supplier that has more than 250,000 customers. For the financial services sector, it is the large banks, the payment systems and the Bank of England (which is also a payment system). Q28 [Jonathan Brearley, Lyndon Nelson]

[77] Dr Martyn Thomas (CNI0004) paras 3.1–3.2

[78] The section on CNI is included in the "Defend" section of the 2016 NCSS. The other two main sections are "Deter" and "Develop". There is also a fourth element focused on international engagement. Cabinet Office, National Security Secretariat (CNI0013) para 12

- a clearly defined starting point (stating only that "cyber risk is still not properly understood or managed", in place of a differentiated analysis of CNI sectors' cyber maturity);
- a clearly defined end point (stating only that the Government and Devolved Administrations will work to ensure that CNI "are sufficiently secure and resilient in the face of cyber attack", without defining what "sufficiently secure and resilient" means in practical, objective terms); and
- metrics by which progress can be objectively assessed against a set timeframe (stating instead that success will be measured against two, high-level outcomes—(a) that the Government understands the level of cyber security and has measures in place to intervene, and (b) that CNI operators understand the level of threat and have implemented proportionate cyber security practices).[79]

As such, it is difficult to tell from the 2016 NCSS precisely what the Government wants to achieve in relation to CNI, over what timeframe or how it intends to assess progress along the way. It is also difficult to tell on what basis, therefore, the Government keeps its "strategic objectives and the balance of investment and activity from HMG under continual review".[80]

29. This lack of detail may be explained in part by a lack of agreed understanding on how best to describe or quantify risk and mitigation in relation to cyber security. The civil nuclear regulator, the Office for Nuclear Regulation (ONR), highlighted the need for "A simple commonly accepted basis for expressing exposure to cyber security risk across the critical national infrastructure", which would enable effective comparison between CNI sectors and a more consistent approach by the Government, operators and regulators.[81] Yorkshire Cyber Security Cluster stated that research into appropriate and useful metrics "must be encouraged as a matter of urgency".[82] When we asked the Government how it was measuring progress against the 2016 NCSS objectives, Ciaran Martin told us that

> cybersecurity, despite its grounding in modern technology, has been the subject of relatively small amounts of performance data internationally, so we are seeking to develop those performance measures.[83]

He pointed to the information included in the NCSC's latest Annual Review and in the February 2018 annual report on Active Cyber Defence (ACD) as a way in which the Government is "seeking to move the debate on".[84]

[79] HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, paras 5.4.2–5.4.3, 5.4.10

[80] Cabinet Office, National Security Secretariat (CNI0013) para 17

[81] The Office for Nuclear Regulation (ONR) states that the reasons for this are "allied to many of the issues associated with cyber risk in general: the complexity and interconnected nature of modern digital systems, the range and diversity of adversary capabilities and motives, and the continual pace of developments." Office for Nuclear Regulation (CNI0031) paras 7, 40

[82] Yorkshire Cyber Security Cluster (CYB0015) para 3.4

[83] Q55 [Ciaran Martin]

[84] Q55 [Ciaran Martin]. See paragraph 40 for further information on Active Cyber Defence.

Transparency of 2016 NCSS implementation

30. The main vehicle for implementing the 2016 NCSS is the 2016–2021 National Cyber Security Programme (NCSP), a five-year programme of cross-government activity which includes initiatives to build the cyber security of CNI.[85] Its budget of £1.9 billion over five years is more than double that of the first NCSP (2011–2016), which stood at £860 million[86]—a significant uplift which was described by techUK as an indicator of "how seriously the Government is taking cyber security".[87]

31. The total budget is the only information about the 2016–2021 NCSP consistently published by the Government. This is in stark contrast to the Government's previous practice of publishing Annual Reports on the delivery of the 2011 NCSS, which—although high-level in nature—included progress updates on key objectives and a breakdown of expenditure by types of activity, such as "National Sovereign capability to detect and defend high end threats" and "Education and skills".[88] While the NCSC's Annual Reviews provide some information about NCSP expenditure—not least because the NCSC is itself partly funded under the NCSP—these documents provide only a snapshot of activity across Government.[89] Many departments and agencies receive NCSP funding but this is not readily identifiable in their own Annual Reports and Accounts.

32. When we put this lack of transparency to David Lidington, he told us that

> while there would certainly be some elements of that £1.9 billion that, while important, might not merit the highest degree of classification, the more information we give which allows both criminals and hostile state actors to subtract from the £1.9 billion and work out what we might be spending elsewhere and what that sum might be buying us, the more the risk increases.[90]

33. We accept that the sensitivity of some NCSP activity means that particular elements cannot be publicly disclosed. However, the Government's unwillingness to publish even basic information about the NCSP hinders external scrutiny of the effectiveness and value for money of the 2016 NCSS and the NCSP.[91] It also has the practical effect of making it difficult for the private sector to understand the Government's priorities,[92] despite the essential nature of this partnership to building CNI resilience to cyber attack.[93]

[85] Cabinet Office, National Security Secretariat (CNI0013) para 24

[86] Cabinet Office, National Security Secretariat (CNI0013) para 13; Cabinet Office, "The UK Cyber Security Strategy 2011–2016: Annual Report", April 2016, p. 5

[87] techUK (CNI0015) para 32

[88] See, for example, Cabinet Office, "The UK Cyber Security Strategy 2011–2016: Annual Report", April 2016. The breakdown of funding by type of activity under the NCSP is available in Annex A.

[89] Q56 [Ciaran Martin]; NCSC, "Annual Review 2017", October 2017; NCSC, "Annual Review 2018", October 2018

[90] Q56 [David Lidington MP]

[91] In September 2016 the National Audit Office reported on the activities of the NCSC and the NCSP in relation to the Government's protection of data. National Audit Office, Session 2016–17, *Protecting information across government*, HC 625

[92] techUK (CYB0021) para 5.5; Information Assurance Advisory Council (CYB0008) paras 2(a)(vii), 8

[93] In written evidence to the inquiry, the Cabinet Office stated: "Effective protection of CNI from cyber attack is a priority for Government and must be a partnership between Government, regulators and private-sector operators." Cabinet Office, National Security Secretariat (CNI0013) para 27

34. **The 2016 National Cyber Security Strategy states that ensuring the resilience of the UK's critical national infrastructure to cyber attack is a priority for the Government. But the Strategy does not set out (a) what specifically the Government wants to achieve; (b) over what timeframe; or (c) how it intends to measure progress. We are therefore concerned that despite the designation of major cyber attacks as a top-tier threat to UK national security, the Government does not have clearly defined objectives for the five-year period covered by the Strategy nor a structured plan for delivering them. This echoes our findings specifically in relation to cyber security skills, which we set out in our July Report.**

35. **The Government is unwilling to publish any information about the 2016–2021 National Cyber Security Programme other than its total budget of £1.9 billion. While we accept that some elements of the NCSP are security-sensitive and therefore should not be made public, such lack of transparency about such large sums of public money is of serious concern. It is also a backwards step, given that the previous Government published Annual Reports and high-level budget breakdowns by activity for the earlier 2011–2016 NCSP.**

36. ***The Government should resume publishing Annual Reports for the National Cyber Security Programme to improve transparency and aid external scrutiny. These should set out progress made, the challenges faced, and a breakdown of the budget by type of activity and by department or agency; it would also present a regular opportunity to review and adjust plans in response to changing threats, vulnerabilities and technological innovation (as we concluded in paragraph 19). Given the relatively large sum of public money and the many departments and agencies involved, the Government should also support a programme-wide audit of the NCSP by the National Audit Office to provide public and Parliamentary assurance.***

4 Building CNI cyber resilience: getting ahead and staying ahead

An "expanded role" for the Government on CNI?

37. In the 2016 NCSS, the Government sets out a clear division of responsibility for ensuring the cyber resilience of CNI:

- CNI operators (whether public- or private-sector) are responsible for identifying and managing the cyber risk to the CNI assets that they own and operate;
- regulators (where identified) are responsible for providing assurance that CNI operators are taking "appropriate" measures to manage cyber risk to their operations; and
- the Government (via the lead Government departments for each CNI sector and the NCSC) is responsible for setting the policy and regulatory framework for CNI operators and regulators, providing threat intelligence to guide their efforts, and providing a point of engagement and collaboration with other countries.[94]

Many of those who provided evidence considered this a natural division of responsibility that also takes account of the importance of public-private partnerships in managing cyber risk, given that the majority of CNI is privately owned.[95]

38. However, as we noted in Chapter 3, the 2016 NCSS explicitly acknowledges that the key assumption underpinning the 2011 Strategy—that the private sector, including CNI operators, would be incentivised by consumer demand and the potential costs of a successful cyber attack to protect its own systems—is fundamentally flawed. It explains:

> the combination of market forces and government encouragement has not been sufficient in itself to secure our long-term interests in cyberspace at the pace required. Too many networks, including in critical sectors, are still insecure. The market is not valuing, and therefore not managing, cyber risk correctly.[96]

The Government acknowledges that, as a result,

> cyber risk is still not fully understood and managed across much of the CNI, even as the threat continues to diversify and increase.[97]

39. This suggests that the Government must now do more to ensure that all CNI operators, and especially those that are privately-owned, "manage their cyber risk in the national interest"—that is, that they put national security interests before business interests where

[94] Lead Government departments are required to publish sector resilience plans for their respective sectors. HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, paras 5.4.7–5.4.8; Cabinet Office, National Security Secretariat (CNI0013) para 35; Q59 [David Lidington MP]

[95] Palo Alto Networks (CNI0011) para 31.1.1; CrowdStrike (CNI0014) para 6; The International Institute for Strategic Studies (CNI0017) para 6; BT Group (CNI0018) para 7.1; Aerospace, Defence, Security & Space (CNI0020) para 1.10; Nokia (CNI0022) para 6.1

[96] HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, paras 4.12–4.13

[97] Cabinet Office, National Security Secretariat (CNI0013) para 37

they do not align.[98] As University of Oxford cyber security researcher Jamie Collier pointed out, this is particularly important given that the costs and consequences of a major cyber attack on CNI, such as a power grid outage, "would fall on citizens rather than the relevant private owners".[99]

40. The 2016 NCSS certainly sets the expectation that the Government will assume an "expanded role" in addressing this market failure and "driving change" across the economy.[100] Yet despite describing it as a priority,[101] the Government's efforts specifically in relation to CNI in the two years since the Strategy was published appear to have been limited.[102] The Government's most significant achievements so far have been:

- the creation of the NCSC—a national technical authority on cyber security (and public-facing part of GCHQ) that provides a single source of advice for the Government and private sector.[103] The evidence indicates this has been an important and successful step. According to the Government, the NCSC's creation has "significantly improved consistency in the cyber security standards and guidance applied across Government and CNI operators".[104] Witnesses have also generally welcomed the NCSC's efforts in relation to CNI, describing the development of a positive and productive working relationship.[105] There are concerns, however, about the capacity of the NCSC to provide close and sustained support to CNI operators and regulators (which we discuss in Chapter 5);

- establishing the Active Cyber Defence (ACD) initiative, which aims to protect the UK from high-volume commodity attacks by stopping them before they reach end users.[106] So far the NCSC has piloted four ACD tools in one CNI sector—'government' (although not all public-sector networks have been included)—describing it as a "great success".[107] The Government's "long term goal" for ACD is to "encourage" these services to be adopted by other CNI sectors in the UK,

[98] Jamie Collier (CNI0006) paras 2.1–2.2; Cabinet Office, National Security Secretariat (CNI0013) para 14; techUK (CNI0015) para 27. Some witnesses suggest it is unrealistic or even "irresponsible" of the Government to expect privately-owned companies to privilege national security over their commercial obligations to shareholders. They also pointed to the traditional role of the state in defending the country against other state actors. Manchester Metropolitan University (CNI0001) para 5.4; Dr Martyn Thomas (CNI0004) para 6.1; Glasswall Solutions Limited (CNI0007) paras 5.1–5.2

[99] Jamie Collier (CNI0006) para 2.2

[100] HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, paras 4.15–4.17

[101] Cabinet Office, National Security Secretariat (CNI0013) para 33

[102] Manchester Metropolitan University observes that there was "so much promise of action [under the 2016 NCSS], with so little eventual substance". Manchester Metropolitan University (CNI0001) para 4.1

[103] HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, para 4.16

[104] Cabinet Office, National Security Secretariat (CNI0013) para 36

[105] Q36 [Lyndon Nelson, Paul Smith]; Manchester Metropolitan University (CNI0001) para 4.6; Jamie Collier (CNI0006) paras 3.3, 7; Palo Alto Networks (CNI0011) para 12; Chatham House (CNI0012) paras 2.1, 2.3; techUK (CNI0015) paras 36–39; Aerospace, Defence, Security & Space (CNI0020) paras 1.11–1.12; Nokia (CNI0022) para 5.2

[106] There are four main services that at a high level involve: spotting website weaknesses; blocking access to malicious sites; taking down malicious content; and blocking fake emails. BT Group described the ACD programme as a "major learning point" addressed in the 2016 NCSS. BT Group (CNI0018) para 4.1; NCSC, *Active Cyber Defence: one year on*, 5 February 2018; NCSC, "Annual Review 2018", October 2018, p. 14.

[107] The NCSC's 2018 Annual Review provides data for progress made under the ACD initiative so far in, for example, reducing the UK's share of identified global phishing attacks from 5.3% (June 2016) to 2.4% (June 2018) and reducing the availability time for sites spoofing Government brands from 42 hours (2016) to 10 hours (2018). The review also shows an increase in the number of public-sector organisations using the service over the last year. NCSC, "Annual Review 2018", October 2018, p. 15

having declined so far to make its implementation mandatory.[108] [109] Some CNI operators have already adopted similar tools;[110] however, others have asked for the Government to offer more protective controls as a service;[111] and

- the implementation of new regulations for some CNI sectors under the EU's Network and Information Systems (NIS) Directive, agreed by the European Parliament in July 2016.[112] Although this suggests a more robust approach to regulation on the part of the Government, it was mandatory for the UK, as an EU member state, to implement the NIS Directive. There are also reasons to doubt whether the new regulations will achieve the required leap forward in cyber resilience (see paragraph 49).

41. The Government's own 2016 review of regulation and incentives relating to cyber security suggested that there is much more that it could be doing.[113] [114] Options range from softer measures such as facilitating information-sharing, to more robust regulation imposing legal obligations on CNI operators, to legislation establishing "an offence of gross neglect in regards to computer infrastructure, particularly as it relates to CNI"—an option suggested by Manchester Metropolitan University.[115] Not all these measures would be suitable or effective immediately. Noting a potential for unintended consequences from Government interventions more generally, Pete Cooper suggested that pursuing "a mix of approaches is probably the most productive".[116]

42. But the Government will first need to understand why many private- and public-sector operators have so far failed to prioritise investment in cyber resilience if it is to identify effective incentives and interventions.[117] Ciaran Martin told us that although work had begun on establishing where operators' commercial interests align with national security interests, and what happens when they do not, there is "more work" to do.[118] Only then will the Government be able to identify how best to drive up the resilience of CNI in all sectors, while also establishing the structures and culture that will encourage CNI operators to increase their resilience to changing threats and new vulnerabilities in the long term.

[108] The NCSC has no enforcement powers to require operators to take specific cyber security actions.

[109] The NCSC Annual Review states: "We pilot our ACD tools with the public sector first and, where relevant, demonstrate the benefits to other sectors. This year, we are working with a range of companies and departments to understand how we can help different sectors. We are also encouraging a range of technology providers to offer similar services to their customers". NCSC, Annual Review 2018, October 2018, p. 15

[110] BT Group (CNI0018) para 4.1; Q6 [Peter Gibbons, Rob Shaw]

[111] Water UK suggested that the Government could to more to offer more protective controls as a service, Q37, Water UK (CNI0027) para 18

[112] Directive (EU) of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (2016/1148); Network and Information Systems Regulations 2018 (SI 2018/506)

[113] HM Government, *Cyber Security Regulation and Incentives Review*, December 2016

[114] The United States' 2018 National Cyber Strategy also cites incentivising investment as a priority. White House, *National Cyber Strategy*, September 2018, p. 9

[115] Manchester Metropolitan University (CNI0001) para 5.6

[116] Pete Cooper (CNI0019) para 13

[117] Witnesses cited the 2017 WannaCry attack as evidence that it is not just private-sector operators that face difficult decisions in trying to balance business needs with investment in cyber resilience, even though the public sector has no commercial obligations. Q14 [Rob Shaw]; Jamie Collier (CNI0006) para 3.2

[118] Q60 [Ciaran Martin]

43. **The Government's current approach to improving the cyber resilience of the UK's critical national infrastructure is long on aspiration but short on delivery. Establishing the National Cyber Security Centre as the national technical authority and introducing more robust regulation for some CNI sectors were both important steps. The latter was mandatory for the UK as an EU member state, however. It appears that the Government is reluctant to move more forcefully and, by default, continues to rely on market forces to improve operators' cyber resilience, despite recognising the previous failure of this approach. Its efforts so far certainly fail to do justice to the status of major cyber attacks as a top-tier threat to national security or to the importance of CNI to the economy. Greater urgency is required if the UK is to 'get ahead' and 'stay ahead' of the cyber threats to its CNI.**

44. ***As we concluded in relation to cyber security skills in our July Report, the Government must first understand the problem before it can address it. The Government should therefore immediately commission work to understand how and why the market has failed to deliver improved cyber resilience of CNI in both the public and private sectors. Only then will it be in a position to identify the targeted interventions and incentives—whether regulatory or otherwise—that will drive up cyber resilience of CNI, while also establishing the culture and practices necessary for continual improvement in the long term.***

Regulation: fixing market failure by setting a higher benchmark

45. Under the Government's previous policy of 'light touch' regulation,[119] only a handful of CNI sectors had regulators with specific statutory powers to assure operators' cyber resilience (see Box 1). This has resulted in what the Government described as a "mixed" regulatory landscape, with the civil nuclear and financial services sectors possessing strong regulatory frameworks and other sectors lacking "backstop powers to intervene" or "clear cyber security standards", or both.[120]

[119] Cyber security researchers Jamie Collier and Pete Cooper both argue that organisations' failure to invest sufficiently in cyber resilience in the years up to 2016 proves that this "hands-off approach" to regulation failed. Jamie Collier (CNI0006) para 3; Pete Cooper (CNI0019) para 12

[120] Cabinet Office, National Security Secretariat (CNI0013) para 39

Box 1: Regulatory landscape before May 2018

Before the NIS Regulations came into force, regulation of CNI sectors could be broadly divided into economic regulators tasked with overseeing market competition issues (for example, the energy regulator Ofgem and the water regulator Ofwat) and regulators with statutory powers specifically to oversee safety and security practices (for example, the Office for Nuclear Regulation). Since 2011 Ofcom has acted as both an economic and security regulator, with telecommunications providers required under UK law to take measures to protect the security and resilience of their networks. The three financial services regulators—the Bank of England, Financial Conduct Authority and Prudential Regulation Authority—have collectively focused on ensuring the resilience of the financial system. As the security trade association ADS observes, the extent to which many of these regulators had a formal role in overseeing the cyber security arrangements of privatised industries was unclear. This was especially the case for the economic regulators whose responsibility for price controls involved assessing the funding that CNI operators needed to manage cyber risk, but did not give specific powers to intervene if those measures applied were not "appropriate" to the risk.

Source: Q26 [Jonathan Brearley, Steve Unger]; Aerospace, Defence, Security & Space (CNI0020) para 1.114; Ofcom, Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003, 18 December 2017

46. In February 2018 the Government told us that it was committed to ensuring that there are "effective regulatory frameworks" in place.[121] In May 2018 the UK brought into force the EU-wide NIS Directive,[122] through the Network and Information Systems Regulations 2018 (Box 2).[123] According to the Government, the NIS Regulations will drive "a consistency of approach and [level] up standards by introducing requirements in an appropriate and proportionate manner".[124] David Lidington told us that the aim of the new regulatory framework is not to "impose penalties", but to "drive change in behaviour and alertness among the operators".[125]

[121] Cabinet Office, National Security Secretariat (CNI0013) para 38

[122] The EU-wide General Data Protection Regulation (GDPR) also came into force in the UK in May 2018, under the Data Protection Act 2018. It is designed to modernise laws that protect the personal information of individuals. GDPR applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location. This therefore includes UK CNI operators. Information Commissioner's Office, *Guide to the General Data Protection Regulation*, 22 March 2018

[123] Network and Information Systems Regulations 2018 (SI 2018/506)

[124] Cabinet Office, National Security Secretariat (CNI0013) para 41

[125] Q59 [David Lidington]

Box 2: The Network and Information Systems Regulations 2018

The purpose of the NIS Regulations is to improve the security of certain industry sectors that provide essential services, with an emphasis on ensuring continuity of service. They do so by, among other provisions:

- requiring operators to implement "appropriate and proportionate" security measures—including in areas such as governance—and setting statutory enforcement mechanisms accordingly;
- establishing 'Competent Authorities' (regulators) for each of the sectors covered by the regulations, to ensure ongoing compliance;
- identifying a 'Single Point of Contact' within Government for engagement with other EU Member States—which is the NCSC in the UK's case; and
- establishing a national 'Computer Security Incident Response Team' (CSIRT)—also the NCSC in the UK.

The regulations apply to the drinking water, energy, health, transport and digital infrastructure (communications) sectors, as well as certain digital service providers that fall outside the UK Government's definition of 'critical national infrastructure' (see Chapter 3 for a discussion of the definition of CNI). The banking and finance sector is exempt from the NIS Regulations, despite being designated in the EU Directive, because equivalent regulation already exists under other UK legislation. The regulations set a threshold—for example, the number of customers served—to specify which operators in each sector are considered "essential services" within the scope of the regulations. About 500 operators of essential services and 200 digital service providers in the UK are expected to fall within the scope of the NIS Regulations.

When implementing security measures, operators within the scope of the NIS Regulations are required to follow guidance issued by the relevant Competent Authority. The fourteen cyber security principles set by the NCSC on behalf of the Government have been adopted by many of the Competent Authorities as a basis for their regulatory approach.

The NIS Regulations also make it mandatory for operators to report incidents whose impact exceeds the threshold set by the relevant Competent Authority "without undue delay and in any event no later than 72 hours after the operator is aware that a NIS incident has occurred".

Although the Government describes fines under the legislation as a "last resort", organisations that fail to implement effective cyber security measures could be fined up to £17 million.

Source: Network and Information Systems Regulations 2018 (SI 2018/506); NCSC, "Table view of principles and related guidance", accessed 24 October 2018; Q59 [David Lidington MP]

47. It is too early to assess the impact of the NIS Regulations, which have been in force for only six months. The Government's own assessment is that it will take at least a couple of years for the Regulations to take full effect.[126] Nevertheless, many of those who provided written evidence welcomed the introduction of tougher regulation in general, and of the NIS Regulations specifically, as a way of setting a higher benchmark for cyber risk management across some CNI sectors as well as digital service providers.[127] In particular, the move away from prescriptive standards towards a focus on outcomes under the NIS Regulations was welcomed because:

- standards are soon rendered out-of-date by fast-changing threats and the frequent discovery of previously unknown vulnerabilities;[128] and
- a risk management approach encourages CNI operators to understand the specific threats to their operations, to think proactively and holistically about how they manage their cyber risk and, ultimately, to anticipate fast-changing threats instead of slipping into a 'tick-box compliance' with static standards.[129] [130]

48. However, some witnesses expressed concern that moving to stronger regulatory oversight risks jeopardising the necessary collaboration and information-sharing between operators, regulators and the Government,[131] which were described as essential to sustaining resilience to fast-changing threats.[132] Ofgem's Jonathan Brearley argued that the NIS Regulations must therefore be implemented in a way that still encourages operators to be "very transparent about their problems", by avoiding an overly punitive approach.[133]

[126] The Government has advised Competent Authorities to take a "cautious approach to enforcement" in the first year while the designated operators of essential services adjust to the new expectations and the NCSC is still developing the Cyber Assessment Framework ('Indicators of Good Practice') which will likely inform many Competent Authorities' early approach to the implementation of the NIS Regulations. The Government is also required to publish a review of the regulations by 9 May 2020, two years after they first came into force. Department for Digital, Culture, Media and Sport (DCMS), *Security of Network and Information Systems: Guidance for Competent Authorities*, April 2018, p. 23; Q59 [David Lidington MP]; *Network and Information Systems Regulations 2018*, Regulation 25.

[127] NCC Group (CNI0002) para 2.3.1.3; Nettitude (CNI0003) para 21; techUK (CNI0015) para 46; Aerospace, Defence, Security & Space (CNI0020) para 1.15

[128] Pete Cooper (CNI0019) para 12; Red Hat Inc (CNI0021) para 5; Corero (CNI0023) para 11; Q37 [Jonathan Brearley]

[129] Q27 [Jonathan Brearley]; NCC Group (CNI0002) para 2.3.2.1; techUK (CNI0015) para 9; Pete Cooper (CNI0019) Executive Summary, para 12; Aerospace, Defence, Security & Space (CNI0020) para 1.15; UKCloud Ltd (CNI0024) para 3.3; Office for Nuclear Regulation (CNI0031) para 13

[130] The United States' 2018 National Cyber Strategy also states that it will work with the private sector to implement a "risk-management approach". White House, *National Cyber Strategy*, September 2018, p. 8

[131] Q32

[132] The International Institute for Strategic Studies (CNI0017) para 6. They are also the hallmarks of the more mature regulatory approaches taken by the financial services and civil nuclear sectors. Q59 [Ciaran Martin]; Office for Nuclear Regulation (CNI0031) paras 5–6, 15

[133] Q26 [Jonathan Brearley] The Government also states that collaboration between regulators and industry must continue. Cabinet Office, National Security Secretariat (CNI0013) para 13

49. Witnesses also cited three significant factors that could diminish the impact of the NIS Regulations in setting a higher benchmark for cyber resilience:

i) several CNI sectors still do not have a regulator with statutory powers to assure operators' cyber resilience.[134] The Government has said it will introduce regulatory regimes for non-NIS sectors and that these sectors will benefit in the meantime from the standards and guidance being developed in support of the NIS Regulations.[135] The failure to include these sectors in the initial implementation of the NIS Regulations is regrettable. In addition, witnesses believed that the current scope of the NIS Regulations does not adequately account for the interconnected nature of the UK economy and its CNI sectors,[136] and suggested that the Regulations be extended to areas "below" CNI such as manufacturing;[137]

ii) the regulatory landscape established under the NIS Regulations is still fragmented, and is complicated by the introduction of joint 'Competent Authorities'.[138] [139] The creation of multiple, sector-specific Competent Authorities under the NIS Regulations reflects a pre-existing division of responsibilities, with lead Government departments (in Whitehall and in the Devolved Administrations) responsible for the operational resilience of CNI in their policy areas but working in collaboration with sector regulators and relevant technical authorities.[140] While this regulatory structure allows for differentiation between sectors according to their needs, it also acts as a potential barrier to cross-sector benchmarking, collaboration and learning—and therefore to cross-sector coherence;[141] and

iii) there is mixed capacity among regulators (Competent Authorities and non-NIS regulators) to provide assurance and support to CNI operators,[142] [143] with newly designated Competent Authorities now embarking on a "steep

[134] In addition to the five CNI sectors covered by NIS (see Box 2), the financial services and civil nuclear sectors are covered by equivalent or better regulatory frameworks established under pre-existing legislation. Cabinet Office, National Security Secretariat (CNI0013) para 39
This leaves the chemicals, defence, emergency services, food, government and space sectors out of scope.

[135] Cabinet Office, National Security Secretariat (CNI0013) paras 41–42

[136] Professor Chris Johnson, writing on behalf of the UK Computing Research Committee, noted that the compromise of regional airports—which are currently excluded from the NIS Regulations—would have a knock-on impact on "core" infrastructure. UK Computing Research Committee, UKCRC (CNI0005) para 6

[137] NCC Group (CNI0002) para 2.1.3.4; techUK (CNI0015) para 1.15; Aerospace, Defence, Security & Space (CNI0020) para 1.1.8

[138] Q18 [Rob Shaw]. Ofcom's Steve Unger argued that: "Clearly, different approaches have been taken in different sectors, but the most important thing is that in any given sector it is clear who is responsible." Q34 [Steve Unger]

[139] These joint Competent Authorities are often between a lead Government department and an existing regulator. The list of Competent Authorities is set out in Schedule 1 of the Network and Information Systems Regulations 2018 (SI 2018/506).

[140] Cabinet Office, National Security Secretariat (CNI0013) para 28; Q34 [Jonathan Brearley]

[141] NCC Group (CNI0002) para 2.3.1.1; Nettitude (CNI0003) para 15; Jamie Collier (CNI0006) para 6; Pete Cooper (CNI0019) para 14

[142] Dr Martyn Thomas (CNI0004) para 5.2; UK Computing Research Committee, UKCRC (CNI0005) para 17; Palo Alto Networks (CNI0011) paras 16–17, 27; techUK (CNI0015) para 50

[143] The UK has established eleven Competent Authorities, based on a sector-by-sector approach. Competent Authorities have powers to issue information notices, carry out inspections, issue enforcement notices and issue penalty notices. The intention is that Competent Authorities will not only enforce the NIS Regulations, but will also be able to assist operators in understanding threats and risks to their respective operations and establish a system-wide view of threats and risks. DCMS, *Security of Network and Information Systems: Guidance for Competent Authorities*, April 2018; Q26 [Jonathan Brearley, Lyndon Nelson]

learning curve".[144] [145] As our July Report on cyber security skills described, some have found it extremely difficult to recruit the expertise they now need.[146] The stated intention of some regulators to rely on the NCSC for technical advice and support also raises important questions about the NCSC's own capacity to provide such support alongside its many other duties (see Chapter 5).[147]

50. Many of the regulators that provided evidence took the view that ensuring consistency, collaboration and learning between CNI sectors was their collective responsibility, via cross-sector forums such as the UK Regulators Network.[148] Yet there is also a role for central Government in promoting consistency and facilitating the sharing of best practice across sectors,[149] at least in the short term. The NCSC is convening workshops for Competent Authorities, in addition to providing common standards and guidance.[150] The ONR suggested that this cross-sector activity might be extended to the active development of "joint approaches" to shared problems[151]—a much more ambitious goal.

51. **The Network and Information Systems Regulations offer a more robust regulatory framework for many CNI sectors, especially in making it mandatory for operators to report incidents where their impact exceeds a predetermined threshold. Although these regulations have only recently come into force, we expect them to set a higher benchmark for cyber risk management in those CNI sectors where they apply. They should also, we hope, foster a culture of proactive and continual risk management by CNI operators, moving away from a 'tick-box compliance' approach.**

[144] Water UK (CNI0027) para 8

[145] For example, Ofgem's role was previously limited to enforcing economic regulation in the energy sector but it is now assuming regulatory responsibility for the sector's cyber resilience, albeit jointly with the Department for Business, Energy and Industrial Strategy. Q26 [Jonathan Brearley]
Ofcom is also assuming additional regulatory responsibility for cyber risk management in the telecommunications sector under the NIS Regulations. Q26 [Steve Unger]

[146] Joint Committee on the National Security Strategy, Second Report of 2017–19, *Cyber Security Skills and the UK's Critical National Infrastructure*, HL Paper 172, HC 706, paras 11, 15; Q27 [Jonathan Brearley, Steve Unger]. This is due in part to the highly competitive salaries offered by elements of the private sector. Q50 [Dr Alastair MacWillson]

[147] Q27 [Jonathan Brearley]; Palo Alto Networks (CNI0011) paras 17, 26
The UK Computing Research Committee observes that the NCSC itself "lacks the human resources required to fully support all government departments and regulatory organizations involved in CNI". UK Computing Research Committee, UKCRC (CNI0005) paras 10–11

[148] Qq34–35 [Jonathan Brearley, Steve Unger]; Financial Conduct Authority (CNI0033) para 10.2. Paul Smith, representing the water trade body Water UK, was also of this view. Q34 [Paul Smith]; Water UK (CNI0027) paras 13–14
In the 2018 Budget the Government stated that the UK Regulators Network will publish a plan in spring 2019 outlining how it will improve collaboration between regulators. HM Treasury, *Budget 2018*, HC 1629, 29 October 2018, para 4.31

[149] Pete Cooper (CNI0019) para 14; Red Hat Inc (CNI0021) para 30

[150] Cabinet Office, National Security Secretariat (CNI0013) para 36; Office for Nuclear Regulation (CNI0031) para 33

[151] For example, identifying critical digital assets in complex industrial control systems. Office for Nuclear Regulation (CNI0031) para 33

52. **Nevertheless, the NIS Regulations are not a 'silver bullet':**

- **the NIS Regulations are limited in scope, leaving some CNI sectors still without statutory regulation and enforcement powers for cyber risk management;**
- **the fragmented responsibility for the NIS Regulations' implementation across Whitehall, Devolved Administrations and regulators remains confusing and acts as a barrier to cross-sector consistency and collaboration—in particular, the introduction of joint Competent Authorities in some sectors clouds accountability and effectiveness; and**
- **some designated 'Competent Authorities' currently lack the expertise and capacity to provide credible assurance of operators' efforts—an issue we addressed directly in our July Report on cyber security skills.**

We are therefore concerned that the NIS Regulations will not be enough in themselves to achieve the required leap forward in cyber resilience across all CNI sectors.

Regulatory assurance of cyber risk management

53. A key question is how best to assure operators' management of cyber risk, especially in the absence of agreed metrics for cyber risk and resilience (see paragraph 29). Some witnesses highlighted the potential value of threat- and intelligence-led 'penetration testing' as a technical assurance tool for regulators.[152] [153] While some CNI operators may conduct their own penetration testing—with such services available on a commercial basis—the scheme piloted by the financial services sector (called 'CBEST') is regulator-led and sector-wide. The advantages of this type of regulator-led scheme are:

- it offers a more "proactive" approach to regulatory assurance and can provide clarity on tangible steps that would improve resilience;[154]
- its application is "intelligence-led", sector-specific and tailored to individual operators. Using Government-provided intelligence—alongside commercially available intelligence—to recreate likely threats and scenarios enables operators, regulators and the Government alike to better understand the "real-world" risk and resilience of individual operators and CNI sectors;[155] and
- it offers the potential to improve collaboration and information-sharing between the operator, regulator and the Government through regular interaction, as operators are tested, undertake work to mitigate vulnerabilities found and are then tested again.[156]

[152] Penetration testing is the process of running an authorised, controlled test on an organisation to identify vulnerabilities that an attacker could exploit. Advanced penetration testing also considers organisational factors such as personnel, physical access and incident response plans. CREST (CNI0028)

[153] Nettitude (CNI0003) para 22; NCC Group (CNI0002) paras 2.3.2.2–2.3.2.3; CREST (CNI0028) para 3; Q29 [Lyndon Nelson, Steve Unger]; Bank of England, *Speech: Managing cyber risk—the global banking perspective*, 10 June 2014, accessed 7 November 2018

[154] Q27 [Steve Unger]; Q29 [Lyndon Nelson]. Steve Unger told us that the TBEST pilots have involved creating "mitigation programmes" to address vulnerabilities identified during penetration testing. The programmes are implemented by operators and overseen by regulators.

[155] NCC Group (CNI0002) paras 2.3.2.2–2.3.2.3; Q29 [Lyndon Nelson]

[156] Q29 [Lyndon Nelson]; Bank of England, *Speech: Managing cyber risk—the global banking perspective*, 10 June 2014, accessed 7 November 2018

54. Confidence in the potential of this assurance mechanism is high: the Government is actively leading the roll-out of the scheme to two other CNI sectors,[157] and organisations such as the industry accreditation body CREST urged its further extension across all CNI sectors.[158] Some other countries are reportedly adopting similar schemes as part of their own regulatory efforts.[159]

55. However, such tests inevitably provide only a snapshot of an operator's resilience at a particular moment in time, against a particular set of threats.[160] In addition, penetration testing undertaken in the UK is limited to "legal and ethical means" of attack, potentially limiting the authenticity—and therefore the usefulness—of the simulation and its outcomes. For example, the Computer Misuse Act 1990 requires explicit authorisation from the operator and all those suppliers whose services may be touched upon during the simulation, while there are both legal and ethical barriers to targeting employees' private lives as a means of breaching the operator's outer perimeter.[161] Those conducting real cyber attacks would obviously not face such constraints. And the evidence further suggests that there are a number of obstacles to a swift roll-out of penetration testing across CNI sectors:

- such schemes are still very much in their "infancy",[162] and there is "still a long way to go" in terms of the schemes' development;[163]
- not all regulators currently have the capacity or expertise to implement such a scheme effectively.[164] Equally, some operators' cyber resilience may not yet be sufficiently mature for this type of intelligence-led penetration testing to be useful; and

[157] These sectors are communications and government, and the schemes are known as 'TBEST' and 'GBEST', respectively. Discussion is also reportedly under way about extending the scheme to a fourth sector: civil nuclear. Cabinet Office, "Chancellor of the Duchy of Lancaster speech at the National Cyber Security Centre: 16 October 2018", accessed 24 October 2018; NCC Group (CNI0002) para 2.3.3; Nettitude (CNI0003) para 22; Q27 [Steve Unger]

[158] CREST (CNI0028) para 9. NCC Group and Nettitude both echo this call. NCC Group (CNI0002) para 2.3.2.2; Nettitude (CNI0003) para 22
It should be noted that NCC Group and Nettitude are accredited providers of CBEST testing services; CREST played a key role in the design of CBEST alongside the Bank of England.

[159] CREST (CNI0028) para 3; Q29 [Lyndon Nelson]

[160] Dr Martyn Thomas also pointed to the coding errors, and therefore vulnerabilities, that remain in products and devices that have passed thorough testing processes. He therefore concluded: "In the light of the demonstrated ineffectiveness of testing in finding the majority of errors, the fact that a system has passed penetration testing should therefore provide little confidence that it is secure against cyberattack." Dr Martyn Thomas (CNI0004) paras 3.5–3.6

[161] The PRA's Lyndon Nelson said that the restrictions to "legal and ethical means" most greatly affected the first part of penetration testing, which is an attempt to penetrate the "external barrier", to see if an attacker could gain access to the operator's systems and networks. It has fewer implications for the second part of the testing process, which is to explore what an attacker could achieve once the external barrier has been penetrated. (Q30)
NCC Group explained further that the Computer Misuse Act 1990 "deems a person guilty of an offence if they knowingly cause a computer to perform any function with intent to secure unauthorised access to any programme or data held". It consequently called for changes to the Act to facilitate more effective penetration testing. NCC Group (CNI0002) para 2.3.2.2

[162] Q29 [Lyndon Nelson]. Even the most advanced, CBEST, has completed only one round of testing for 34 top-priority organisations.

[163] Q29 [Lyndon Nelson]

[164] This is especially the case for those newly designated Competent Authorities under the NIS Regulations. Water UK's Paul Smith told us that all relevant organisations within the water sector will be expected to undergo penetration testing. However, Ofgem's Jonathan Brearley said that Ofgem is "still scoping up our standard-setting role" and that it would consider penetration testing during this process. Q28 [Paul Smith]; Q29 [Jonathan Brearley]

- there is currently a lack of capacity within the UK's cyber security industry to provide accredited, advanced penetration testing services at scale.[165]

These are all issues which the Government should consider as it seeks to extend regulatory penetration testing across CNI sectors and, crucially, to develop an understanding of the true resilience of the UK's CNI, which is currently lacking. CREST has suggested that the Government create a strategy and detailed implementation plan for doing so.[166]

56. **Threat- and intelligence-led penetration testing shows promise as a mechanism for providing technical assurance of CNI operators' cyber risk management—all the more important in the absence of agreed metrics for cyber risk and resilience. However, such testing should be used in combination with other methods of regulatory assurance because it only provides a snapshot of operational resilience at a particular moment in time against a particular set of threats.**

57. ***The Government should establish a plan (a) for the development of threat- and intelligence-led penetration testing and its roll-out across all CNI sectors that takes account of the mixed maturity of the sectors in terms of their cyber resilience; (b) for the development of the test methodology; and (c) for developing the cyber security industry's capacity to deliver such advanced and accredited testing at scale. It should address the last point in its forthcoming cyber security skills strategy which, as we urged in our July Report, should be published as a matter of priority.***

Regulation after Brexit

58. The Government has said that the NIS Regulations will continue to apply after the UK's exit from the EU.[167] The July 2018 White Paper, *The Future Relationship between the United Kingdom and the European Union*, also states the Government's intention to continue participating in the EU-wide NIS Coordination Group and network of CSIRTs (Box 2)—the formal mechanisms that facilitate the sharing of information about threats and good practice, as well as cooperation on enforcement action and incident response, between EU Member States.[168] Because cyber threats do not stop at national borders, it is also important that the UK continues to support policy development and capacity-building across the EU through the various NIS Coordination Group workstreams and cross-EU exercises.[169] [170]

[165] Q29 [Lyndon Nelson]; CREST (CNI0028) paras 7, 11

[166] CREST (CNI0028) para 9

[167] DCMS, *Security of Network and Information Systems: Guidance for Competent Authorities*, April 2018, section 5.2

[168] HM Government, *The Future Relationship between the United Kingdom and the European Union*, Cm 9593, para 103; Directive (EU) of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (2016/1148); DCMS, *Security of Network and Information Systems: Guidance for Competent Authorities*, April 2018, section 4.7

[169] NCSC, "Annual Review 2018", October 2018, pp. 18, 30

[170] HM Government, *National Cyber Security Strategy 2016–2021*, November 2016; Cabinet Office, National Security Secretariat (CNI0013) paras 52–54. See also NCC Group (CNI0002) paras 2.1.5, 2.3.5; The International Institute for Strategic Studies (CNI0017) para 8; Red Hat Inc (CNI0021) para 14

59. However, whether and how the Government intends to take account of changes made to the NIS regime by the EU after the Brexit transition period ends is unclear.[171] Furthermore, the extent of, and mechanism for, UK participation in EU-wide groups will ultimately be determined by the negotiations on the future UK–EU partnership.[172] In his oral evidence in June 2018, David Lidington declined to comment on future cooperation with the EU in relation to CNI specifically. On the issue of wider security cooperation, he said the Government hopes to overcome "doctrinal issues with the EU institutions", adding that "otherwise, it amounts to a deliberate decision by the EU negotiators to put EU citizens at greater risk than they are at the moment".[173] [174] There is no evidence yet to suggest this impasse has been resolved.

60. **The NIS Regulations will continue to apply in the UK following Brexit. However, the mechanism for UK participation in EU-wide information-sharing and capacity-building is still subject to negotiation.** ***Given that cyber threats do not stop at national borders, the Government should prioritise maintaining access to the EU's NIS Coordination Group and its workstreams to facilitate continued information-sharing and collaboration with EU Member States.***

Cultural change: creating an environment for continual improvement

61. Using regulation to set a stronger framework within which CNI operators must act is only one of the interventions available to the Government. We heard that improving the culture of CNI operators and other relevant organisations is just as important, because this creates an environment in which "improvements are proactively implemented in anticipation of developments and new threats, rather than as a reaction to events".[175] In this regard, witnesses emphasised the fundamental importance of improving day-to-day cyber 'hygiene', which our July Report on cyber security skills identified as a "universal responsibility for all employees".[176] Lyndon Nelson from the Prudential Regulation Authority (PRA) told us, for example, that passwords "are the source of many

[171] This is particularly important if the Government is to reduce the burden of compliance on multinational operators working in other EU member states. ISACA (CNI0010) para 2.1; Aerospace, Defence, Security & Space (CNI0020) para 1.18

[172] DCMS, *Security of Network and Information Systems: Guidance for Competent Authorities*, April 2018, section 5.2; NCC Group (CNI0002) para 2.3.6

[173] Q57

[174] We also heard concerns about the impact of Brexit on other aspects of the UK's collaboration with EU partners on cyber security—for example, through the European Union Agency for Network and Information Security (ENISA). techUK (CNI0015) paras 41–43; ISACA (CNI0010) para 2.2. Witnesses also raised concerns about the impact of Brexit on the UK's access to skills, with some questioning whether immigration policy after Brexit would continue to allow specialist skills to be recruited from the EU and beyond at a time when the cyber security skills shortfall in the UK is "peaking". ISACA (CNI0010) para 3.1.3.1; techUK (CNI0015) para 62; Nokia (CNI0022) para 7.3; Q40 [Ruth Davis]

[175] Office for Nuclear Regulation (CNI0031) para 41. Although the civil nuclear sector is considered to have one of the more mature approaches to sector-wide management of cyber risk, due to longstanding legislation focused on ensuring the safety and security of civil nuclear power, the ONR nevertheless said that "there is still a distance to travel" in this regard.

[176] Joint Committee on the National Security Strategy, Second Report of 2017–19, *Cyber Security Skills and the UK's Critical National Infrastructure*, HL Paper 172, HC 706, para 7

vulnerabilities",[177] while others referred to the need for regular incident response and resilience exercises, cloud storage policies to ensure the safe custody of data, and regular staff training to raise awareness, among other basic steps.[178]

62. Witnesses also raised a number of other non-regulatory interventions aimed at effecting cultural change across CNI sectors and their extended supply chains. Although many of these were discounted by the Government in its December 2016 review of regulation and incentives in relation to cyber security,[179] the rest of this chapter explores those we consider to have the greatest potential in driving cultural change.

Supply chains

63. Supply chains are not formally regarded as part of the UK's CNI, but they are nevertheless integral to their operation. In some cases, third-party companies directly supply a fundamental element of 'critical' services: railway services would not run in the UK without those external suppliers that provide the signalling equipment for Network Rail.[180] Attackers are also increasingly exploiting supply chain vulnerabilities in order to gain access to CNI operators' networks and systems—a development highlighted in the NCSC's latest Annual Review[181]—looking for any points of weakness in their networks.[182] In July, for example, the United States' Department for Homeland Security reported that a Russian state-sponsored group had breached the "control rooms" of US electricity companies by first penetrating the networks of vendors.[183] In addition, the public disclosure of the 'Meltdown' and 'Spectre' security flaws affecting Intel, ARM and AMD computer chips in January demonstrates the potentially pervasive impact of hardware supply chain vulnerabilities.[184]

[177] Q28 [Lyndon Nelson]. See also NCC Group (CNI0002) para 2.1.4; Chatham House (CNI0012) para 4.4

[178] The evidence suggests a number of other basic steps and fundamental good practices that all CNI sectors should be implementing. These include: compliance with basic standards such as Cyber Essentials or ISO 27001; active participation by operators in the Government's Cyber Security Information Sharing Platform (CiSP); sector-wide workshops convened by lead Government departments or regulators to facilitate information-sharing and lesson learning; and staff vetting, as well as phishing trials to raise staff awareness. Q5; Q6 [Phil Sheppard]; Qq8–9; Q28; Q32 [Jonathan Brearley, Paul Smith]; Q51 [Ruth Davis]; Q63; Chatham House (CNI0012) para 4.1; Red Hat Inc (CNI0021) paras 23, 30; UKCloud Ltd (CNI0024); Office for Nuclear Regulation (CNI0031) para 15; Financial Conduct Authority (CNI0033) para 8.2

[179] HM Government, *Cyber Security Regulation and Incentives Review*, December 2016

[180] Network Rail, "Supply of works, services or products", accessed 28 October 2018. Network Rail is the designated operator of essential services under the NIS Regulations, even though it outsources much of the operation of the UK railway services.

[181] The NCSC highlighted the issue of supply chain security in its 2018 Annual Review, stating that it had become "acutely conscious of the role the supply chain plays in leaving organisations vulnerable to compromise". NCSC, "Annual Review 2018", October 2018, p. 11

[182] Nettitude (CNI0003) para 10; techUK (CNI0015) para 21; The International Institute for Strategic Studies (CNI0017) para 8; Nokia (CNI0022) para 6.2

[183] *"Russian hackers reach U.S. utility control rooms, Homeland Security officials say"*, The Wall Street Journal, 23 July 2018

[184] *"Spectre and Meltdown processor security flaws—explained"*, The Guardian, 4 January 2018; The International Institute for Strategic Studies (CNI0017) para 8

64. Witnesses described non-contractual and contractual steps that CNI operators can—and in some cases already do—take to manage the risk with their immediate suppliers.[185] These include:

- assessing whether and how suppliers have access to CNI operator systems, and what implications this access has for cyber security;
- requiring suppliers to undertake regular self-assessment; and
- mandating minimum (or equivalent) cyber security standards for suppliers, such as ISO 27001 or the Cyber Essentials and Cyber Essentials Plus schemes.[186] [187]

The NIS Regulations also set an expectation that CNI operators in the five NIS sectors will ensure that "appropriate measures are employed where third party services are used". These include "contractual agreements" and specified "security properties" for products and services on which "the essential service depends".[188] The Government, meanwhile, is stepping up the cyber security requirements for its direct suppliers, having announced in June that it will write minimum standards into its contracts and create the equivalent to a 'credit rating' for each of its prime suppliers.[189]

65. However, Peter Gibbons of Network Rail told us that the principal challenge in managing what are often long and complex chains is not the operators' direct suppliers, but their suppliers in turn.[190] To meet this challenge, some CNI operators, including the Government, make it the contractual responsibility of the prime contractor to manage and assure risks in its own supply chain.[191] National Grid is more prescriptive in its approach, requiring businesses down its supply chain to undergo the same certification processes as its direct suppliers.[192] [193] TechUK and security trade association ADS both highlight the defence sector's use of cyber risk profiles and associated measures to ensure suppliers are managing risk, wherever they sit in the chain.[194]

[185] Steve Unger and Jonathan Brearley, from Ofcom and Ofgem respectively, told us that it is incumbent on CNI operators to examine their supply chains, undertake an appropriate risk assessment and implement controls accordingly. This is the criteria against which regulators make their own assessment of operators' risk management. Q27 [Steve Unger, Jonathan Brearley]

[186] Q12

[187] NCSC, "Cyber Essentials", accessed 18 September 2018; British Standards Institution (CYB0006) para 6

[188] NCSC, "Guidance: A4. Supply chain", accessed 28 October 2018

[189] *"Government mandates new cyber security standards for suppliers"*, Cabinet Office press release, 26 September 2014; GOV.UK, *Minimum Cyber Security Standards*, June 2018, p. 2; Q59 [David Lidington MP]; Jamie Collier (CNI0006) para 2.1

[190] Q12 [Peter Gibbons]; techUK (CNI0015) para 21

[191] Q59 [David Lidington MP]; Q12 [Rob Shaw]

[192] Q12 [Rob Shaw, Phil Sheppard]

[193] Requiring suppliers at each level of the CNI supply chain to undergo such certification also represents an opportunity to increase the uptake of Cyber Essentials—and therefore to raise the cyber security baseline—across the wider economy. The NCSC's 2017 Annual Review reports that only 7,900 Cyber Essential certificates have been issued since 2014. NCSC, "2017 Annual Review", October 2017, p. 36. Rowland Johnson, Chief Executive of the cyber security company Nettitude, attributes this slow uptake to its optional nature. Nettitude (CNI0003) para 5

[194] The programme is called the Defence Cyber Protection Programme. It was established jointly by the Ministry of Defence and the defence industry in 2013. Its security standards are now based on Cyber Essentials and Cyber Essentials Plus. techUK (CNI0015) para 21; Aerospace, Defence, Security & Space (CNI0020) para 1.7. It should be noted that both techUK and ADS are directly involved in the DCPP.

66. We heard that CNI operators face other, more complex difficulties in managing supply chains risks which would benefit from greater intervention by the Government:

i) it is difficult to mandate and enforce minimum security standards for those products (hardware, software or services) that are bought 'off the shelf', especially where these are procured from major international companies.[195] Consequently, witnesses suggested that the Government should use its "buying power" and diplomatic presence in multinational forums such as the G7 to influence international providers,[196] and potentially establish an NCSC-accredited 'kitemark' for trusted suppliers;[197] and

ii) the widespread use of certain data service providers, software packages, computer processors and hardware creates "single points of failure" that could affect operators simultaneously across CNI sectors.[198] Sean Kanuck, from IISS, argued that the Government should proactively identify these potential points of failure and prepare mitigation and contingency plans.[199]

We explored in our inquiry, and also in our October 2018 evidence session on the National Security and Investment white paper, the role of the Huawei Cyber Security Evaluation Centre Oversight Board in assessing the security of that company's hardware in UK security-sensitive communications networks.[200] ***The Government should set out in its response to this Report its assessment of how, and how effectively, the Huawei Cyber Security Evaluation Centre Oversight Board provides additional assurance in relation to the UK's cyber security.***

[195] The International Institute for Strategic Studies (CNI0017) para 8; UK Computing Research Committee, UKCRC (CNI0005) para 7. As Peter Gibbons stated, "We would not sit down with Microsoft and tell it what our security policies were and what it had to write into its operating systems." Q12 [Peter Gibbons]

[196] Q37 [Lyndon Nelson]

[197] UK Computing Research Committee, UKCRC (CNI0005) para 7; The International Institute for Strategic Studies (CNI0017) para 8; Nettitude (CNI0003) para 12; Q23 [Peter Gibbons]. However, the assurance provided by a kitemark may be limited by the rapid evolution of threats and attackers' capabilities as time passes. The Government has said it is considering several options for introducing a voluntary labelling scheme (kitemark) for consumer Internet of Things devices to "to aid consumer-purchasing decisions and to facilitate consumer trust in manufacturers", further details are expected in spring 2019. DCMS, "Government response to the Secure by Design informal consultation", 14 October 2018, accessed 1 November 2018

[198] The International Institute for Strategic Studies (CNI0017) paras 7–8; UK Computing Research Committee, UKCRC (CNI0005) para 7

[199] The International Institute for Strategic Studies (CNI0017) paras 7–8

[200] Q24 [Peter Gibbons]; Qq26–27 [Steve Unger]; oral evidence taken on 15 October 2018, HC (2017–19) 1634

Corporate governance and reporting

67. The Government places responsibility for managing cyber risk to private-sector CNI operators firmly on the companies' boards.[201] Yet according to techUK—and, indeed, the Government's own assessment—"Cyber risk within CNI is still not fully understood or managed, despite the threat evolving and increasing."[202] [203] As with any other business risk,[204] company boards are expected to show leadership in assessing and managing cyber risk, which often involves making "difficult trade-offs in efficiency, convenience, and other areas related to performance."[205] It is therefore the duty of all board members to "get a little bit more technical"—as Ciaran Martin recently put it—by educating themselves about "the basics … of cyber attacks, cyber risks and cyber defences".[206]

68. There are additional steps that would enable better-informed decision-making and establish a stronger sense of accountability at board level.[207] The NCSC recently published "five questions for boards to get on their agenda" as a starting point for internal conversations, with a view to publishing a more comprehensive "toolkit" for boards later in 2018.[208] While this will no doubt aid those boards that choose to use it, the Government also previously considered—but discounted[209]—making it mandatory for all companies (not just private-sector CNI operators) to identify a board member with specific responsibility for, and expertise in, cyber security. Such a step would ensure that boards have relevant expertise and a clear point of accountability for cyber resilience, covering both technical matters such as defences and cultural aspects such as staff behaviour.[210] [211]

69. A further option would be to mandate corporate reporting on cyber resilience for private-sector CNI operators, which would incentivise boards to focus on understanding and managing cyber risk.[212] This would fit with the spirit of forthcoming reforms to the

[201] Cabinet Office, National Security Secretariat (CNI0013) para 35. Board responsibility is not limited to private-sector CNI operators. Each of the Trusts and Foundations Trusts that make up the NHS is also managed by a board, for example.

[202] techUK (CNI0015) para 25; HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, para 5.4.2

[203] In our July 2018 Report *Cyber Security Skills and the UK's Critical National Infrastructure*, we observed that it is not only deep technical expertise on cyber security that is in short supply, but also "the moderately specialist skills and knowledge required by all those whose jobs have now assumed an important cyber security element—for example … board-level directors who need to understand the cyber risk to business operations". Joint Committee on the National Security Strategy, Second Report of 2017–19, *Cyber Security Skills and the UK's Critical National Infrastructure*, HL Paper 172, HC 706, paras 7, 15

[204] NCSC, "Ciaran Martin's speech at the CBI Conference", 12 September 2018; Office for Nuclear Regulation (CNI0031) para 13

[205] CrowdStrike (CNI0014) para 5

[206] NCSC, "Ciaran Martin's speech at the CBI Conference", 12 September 2018

[207] Q28 [Steve Unger]

[208] NCSC, "Five questions for boards to get on their agenda", 12 September 2018

[209] It did so on the basis that cyber security is a "joint responsibility [shared] across a number of roles". HM Government, *Cyber Security Regulation and Incentives Review*, December 2016, pp. 21–22

[210] Q29 [Lyndon Nelson]

[211] This function might best be performed by a Non-Executive (rather than an Executive) Director, in view of the natural tensions between the commercial interests of private-sector CNI operators and the 'public good' and national security requirements of their operations. Dr Martyn Thomas (CNI0004) paras 6.1–6.2

[212] The Financial Reporting Council, which regulates auditors, accountants and actuaries in the UK, has called for improved corporate reporting on cyber security by all companies. Financial Reporting Council, *Annual Review of Corporate Reporting 2015/2016*, October 2016, p. 32

Companies Act 2006, due to take effect from January 2019.[213] According to an October 2018 PwC report, companies are reluctant to "report insightfully" on cyber security due to concerns that this could increase their vulnerability to attack and potentially leave them open to increased legal or regulatory scrutiny.[214] However, the reporting of non-sensitive information—such as how much time the board has spent discussing cyber resilience, the frequency of third-party testing and incident response exercises, and the number of incidents suffered in a reporting year and the lessons learned[215]—would provide an indication of a board's understanding of operational cyber risk and the extent of its risk mitigation activities. It would also help company shareholders and investors to play what Ciaran Martin recently described as a "stronger role in asking the tough questions" of boards about cyber risk management.[216] [217]

Cyber insurance

70. During our inquiry, we explored whether and how cyber insurance, covering both IT- and OT-related losses,[218] might be beneficial in relation to CNI.[219] According to the Association of British Insurers (ABI), levels of cyber insurance coverage in the UK and EU countries are low by comparison to the US market, which in 2016 accounted for approximately 85% of standalone global cyber insurance premiums.[220] However, the UK market is expected to grow in the coming years, in part due to mandatory data breach reporting under the General Data Protection Regulation (GDPR),[221] and partly in response to the increasing costs of business disruption caused by malware and ransomware attacks.[222] [223]

71. Witnesses offered mixed views on the utility of cyber insurance for CNI. Ofcom's Steve Unger said that he would prefer CNI operators to take "direct responsibly" for cyber resilience, retaining a sense of their own accountability rather than 'outsourcing'

[213] The principal reform is to reporting on compliance with Section 172 of Companies Act 2006. According to the Institute of Directors, under the reforms all large private companies and unlisted plcs must explain in their strategic report—and publish on a website—how the directors have had regard to the matters set out in Section 172 of the Companies Act 2006. Institute of Directors, "Corporate governance reform: an update for directors of private companies", 23 July 2018

[214] Dr Richard Horne, *Transparency in the digital age: companies should talk about their cyber security*, PwC, October 2018. Dr Horne provided oral evidence to our predecessor Committee's inquiry, "Cyber Security: UK National Security in a Digital World" in March 2017.

[215] Dr Richard Horne, *Transparency in the digital age: companies should talk about their cyber security*, PwC, October 2018

[216] "Investors 'must play closer attention' to cyber threat", The Times, 10 April 2018

[217] In its 2016 review of regulation and incentives in relation to cyber security, the Government discounted setting requirements for the public reporting of cyber risk—for example, in annual reports—in the short term at least. The review concludes that "Including information on cyber risk in annual reports is unlikely to be an effective or popular way of encouraging large-scale change in cyber risk management". It did, however, commit to provide guidance to businesses about the type of information on cyber risk that should be included in annual reports and investor reports "in the long term". HM Government, *Cyber Security Regulation and Incentives Review*, December 2016, pp. 20–21

[218] Cambridge Centre for Risk Studies (CNI0025) para 11

[219] In its December 2016 review of cyber security regulation and incentives, the Government declined to set the requirement for cyber insurance despite supporting its uptake. HM Government, *Cyber Security Regulation and Incentives Review*, December 2016, p. 22

[220] ABI (CNI0026) para 1

[221] Fines issued under GDPR are capped at €20 million or 4 percent of global turnover, whichever is greater.

[222] ABI (CNI0026) paras 1–3; Cambridge Centre for Risk Studies (CNI0025) para 13

[223] For example, it is estimated that business disruption caused by the June 2017 NotPetya cyber attack cost the global shipping container company Maersk $250–300 million. Andy Greenberg, *"The untold story of NotPetya, the most devastating cyberattack in history"*, Wired, 22 August 2018

it.[224] The ONR further cautioned that cyber insurance should not be seen as a substitute for regulation, given that the former protects the financial interests of the insured, while regulation acts to protect the public interest.[225] However, other witnesses, including the PRA's Lyndon Nelson, were more positive.[226] One key reason is the potential for cyber insurance to drive cultural change and improve baseline cyber resilience. This might be achieved, for example, through the application process, by ensuring companies regularly assess their cyber risk, or by insurers offering reduced premiums for compliance with basic standards, preferably aligned with regulatory requirements.[227] Another reason is the specialist technical and communications support that insurance companies might offer their customers in responding to a successful cyber attack, with a view to reducing its impact and future vulnerability.[228]

72. We heard that the cyber insurance industry will need to undergo significant development if it is to fulfil its potential, especially in relation to CNI.[229] The most fundamental issue is how to quantify "dynamic" cyber risk accurately and calculate premiums accordingly.[230] [231] There are two principal challenges:

i) the ABI and Lloyd's of London highlighted the lack of historical data which is conventionally used to guide assessments of current and future risk.[232] Lloyd's of London stated that cyber risk poses a "unique challenge" and that "actuarial methods based on history are inappropriate". Consequently, it is seeking to develop new ways of assessing cyber risk;[233] and

ii) according to the Cambridge Centre for Risk Studies, "it is challenging for insurers to fully understand the Operations Technology risks of complex engineering systems and thus harder for them confidently to insure this domain."[234] This in turn has implications for the insurers' willingness to offer cyber insurance for CNI. In large part this is due to their responsibility to regulators to manage aggregation risk—that is, the possibility that many different types of policies will be triggered by the same incident (cyber and property policies, for example) or that the widespread use of the same technology or system by CNI operators (as in the case of WannaCry) will lead to multiple pay-outs.[235]

[224] Q33 [Steve Unger]

[225] Office for Nuclear Regulation (CNI0031) para 30

[226] Q33 [Lyndon Nelson]

[227] ABI (CNI0026) para 10; Financial Conduct Authority (CNI0033) paras 9.1–9.2; Lloyd's (CNI0034) paras 4–5; Cambridge Centre for Risk Studies (CNI0025) paras 15, 18; Office for Nuclear Regulation (CNI0031) para 28

[228] Q33 [Lyndon Nelson]; Financial Conduct Authority (CNI0033) para 9.1; Lloyd's (CNI0034) para 6

[229] Q33 [Paul Smith]; Financial Conduct Authority (CNI0033) para 9.2

[230] Cambridge Centre for Risk Studies (CNI0025) para 18

[231] Other issues cited included the frequent misalignment between policy application questionnaires and established cyber security industry standards, and the lack of clarity about how insurers judge whether a company has been "unlucky or negligent" in the event of a successful cyber attack—and therefore whether to pay out on a policy. Cambridge Centre for Risk Studies (CNI0025) para 16; HM Government, *Cyber Security Regulation and Incentives Review*, December 2016, p. 22

[232] ABI (CNI0026) paras 12–14; Lloyd's (CNI0034) para 3

[233] Lloyd's (CNI0034) para 3

[234] Cambridge Centre for Risk Studies (CNI0025) para 11

[235] ABI (CNI0026) para 5; Cambridge Centre for Risk Studies (CNI0025) para 14. A scenario modelled by the Cambridge Centre for Risk Studies on behalf of Lloyd's, in which the US power grid was subject to cyber attack, estimated a global economic loss of $1 trillion, with a global insurance industry loss of $71 billion in the worst case. Lloyd's, *Business Blackout: The insurance implications of a cyber attack on the US power grid*, May 2015

As such, trade body Water UK summed up the views of many witnesses when it said that the water industry is maintaining "a watching brief" as the cyber insurance industry continues to mature.[236]

73. **A more holistic and effective approach to strengthening the cyber resilience of CNI requires changing the culture of CNI operators and their extended supply chains. Embedding the view that cyber risk is another business risk, which must be proactively managed, will be central to this process. It is especially important for those private-sector operators whose commercial interests may not always align with the demands of national security.**

74. ***The Government should give urgent consideration to non-regulatory incentives and interventions that have the potential to drive cultural change across CNI sectors, establishing an environment in which continual improvement is encouraged. The issues it should consider include:***

- ***how managing cyber risk through and within the extended supply chains of CNI operators could be encouraged;***
- ***how the Government can best support operators in managing cyber risk associated with hardware, software and services bought 'off the shelf', especially those procured from major international suppliers;***
- ***improving board-level expertise and accountability. This includes identifying an expert board member with specific responsibility for cyber resilience and mandatory corporate reporting on cyber resilience, in accordance with the spirit of forthcoming reforms to the Companies Act 2006; and***
- ***how cyber insurance might be used to improve operators' cyber practices, and how the Government can support the market in maturing more quickly.***

[236] Water UK (CNI0027) para 16

5 Leadership within Government

Political leadership: driving change across Government and CNI sectors

75. There is no single Minister with responsibility for the cyber resilience of CNI, or for cyber security in general.[237] Instead, there is a patchwork of cross-cutting ministerial oversight that is structured by department (with lead departments having responsibility for CNI sectors within their policy area), by key strategic objective within the 2016 NCSS, and by the remits of cross-government ministerial committees on national security.[238] (See Box 3 for further detail.) Furthermore, for devolved policy areas, ministerial oversight is split between Westminster and the Devolved Administrations.

76. An advantage of this decentralised structure is that it captures the expertise of departments and allows for policy to be tailored to each CNI sector, with the support of specialist technical agencies and the Cabinet Office.[239] However, focused political leadership is also essential, given the potential extensive impact of a major cyber attack on the UK's CNI and the fast-changing nature of the threat, as well as the need to drive a consistent response across a number of departments and agencies.[240] We have heard little to convince us that there is such a 'controlling mind' at the centre of Government that is proactively leading efforts to improve the cyber resilience of CNI.

77. Ciaran Martin provided the most positive account of the current arrangements, observing that they have delivered "consistently rising funding, strategic stability and the right balance … between organisational autonomy to get on with what we need to do and ministerial sponsorship".[241] He also told us that cyber security is frequently discussed by the National Security Council (NSC) and its sub-committees (Box 3), while the Home Secretary and the Chancellor of the Duchy of Lancaster receive fortnightly briefings from the NCSC on the latest operational threats and NCSC activity.[242]

[237] BT Group stated that it does not even know which part of the Government owns the definition of CNI. BT Group (CNI0018) para 3.1

[238] Q58 [David Lidington MP]; Cabinet Office, National Security Secretariat (CNI0013) paras 18–19, 21, 25

[239] Cabinet Office, National Security Secretariat (CNI0013) para 25; Cabinet Office NSS (CNI0030) paras 6–7

[240] Jamie Collier (CNI0006) para 1.1

[241] Q58 [Ciaran Martin]; Q60

[242] Q58 [Ciaran Martin]

Box 3: Ministerial oversight of the cyber resilience of CNI

Ministerial oversight of cyber resilience is performed concurrently at the departmental, objective-specific, and collective levels.

Departmental ministerial oversight: CNI sectors are assigned to a lead Government department; the respective Secretary of State is therefore responsible for its resilience (Table 1). The Cabinet Office oversees policy relating to, and coordination between, CNI. However, the Minister for the Cabinet Office (currently the Chancellor of the Duchy of Lancaster) does not have overall responsibility for CNI. For devolved matters, the Devolved Administrations have responsibility.

Table 1: Departmental responsibility for CNI sectors

CNI sector	Lead Government department
Chemicals	BEIS
Civil nuclear	BEIS
Communications (including broadcast, internet and post)	DCMS
Defence	MOD
Emergency services	DH&SC and DfT
Energy	BEIS
Finance	HM Treasury
Food	Defra
Government	Cabinet Office
Health and social care	DH&SC
Space	BEIS
Transport	DfT
Water and sewerage	Defra

Source: Cabinet Office, National Security Secretariat (CNI0013) para 25

Objective-specific ministerial oversight: Five Cabinet Ministers have been assigned responsibility for delivering key strategic objectives under the 2016 NCSS (Table 2).

Table 2: Objective-specific ministerial oversight of the 2016 NCSS

Cabinet Minister	Area of responsibility
Home Secretary	Responses to high-category cyber incidents and countering cyber-crime
Defence Secretary	The development of the UK's offensive cyber capability (in collaboration with GCHQ)
Foreign Secretary	The NCSC (as part of his statutory responsibility for GCHQ)
Secretary of State for DCMS	Digital matters, including the relevant growth, innovation and skills aspects of cyber security
Chancellor of the Duchy of Lancaster	Responsible to Parliament for the NCSS and NCSP

Source: Cabinet Office, National Security Secretariat (CNI0013) para 21

Collective ministerial oversight: the cyber resilience of CNI falls within the purview of a Cabinet Committee and two of its sub-committees that focus on cross-government national security policy. These Committees have three different Chairs and meet with varying frequency (Table 3). In 2017 the National Security Council (NSC) sub-committee for cyber security was disbanded, having existed for just over a year.

Table 3: Cross-government ministerial oversight of cyber security and CNI

Cabinet Committee	Committee Chair	Area of responsibility	Frequency of meetings
NSC	Prime Minister	Sets and oversees cross-government cyber security strategy, as part of its responsibility for national security overall	Weekly when Parliament is sitting
NSC (Strategic Defence and Security Review—SDSR) sub-committee	Chancellor of the Exchequer*	Sets and oversees the delivery of the NCSS and NCSP, ensures coherence of cross-government activity on cyber, and holds to account those departments and agencies responsible for delivering NCSS objectives, as part of its responsibility for the delivery of the SDSR	Biannually
NSC (Threats, Hazards, Resilience and Contingencies—THRC) sub-committee	Chancellor of the Duchy of Lancaster	Considers issues relating to security threats, hazards, resilience and contingencies. It provides strategic leadership for the Government's work to prevent, prepare, respond to and recover from the highest-priority risks, including those to CNI	Quarterly

Source: Q58 [David Lidington MP]; Cabinet Office, National Security Secretariat (CNI0013) paras 18–19; oral evidence taken on 6 March 2017, HC (2016–17) 153, Q101 [Amber Rudd MP]; Institute for Government, "Cabinet committees show Damian Green is de facto Deputy PM", 27 July 2017

*When the Cabinet Office submitted written evidence in February 2018, the Home Secretary chaired the NSC (SDSR). The Government announced a change in chairmanship in October 2018. (Cabinet Office, List of Cabinet Committees and their members as at 25 October 2018, accessed 30 October 2018)

78. Other evidence suggests a much more passive approach by Ministers, including:

- varying, generally limited, levels of engagement by the Secretaries of State in their respective CNI sectors;[243]
- infrequent meetings of two of the three Cabinet Committees with responsibility for overseeing cross-government implementation (see Box 3, Table 3);[244] and
- Cabinet Committees having limited discussion of problems that involve more than one department.[245]

[243] Q18; Q38

[244] Q59 [David Lidington MP]; oral evidence taken on 6 March 2017, HC (2016–17) 153, Q101 [Amber Rudd MP]

[245] Q59 [David Lidington MP]

The coherence of political leadership from the centre of Government is further undermined by there being two Ministers with overlapping responsibility for the NCSP's implementation (see Box 3, Tables 2 and 3). The exclusion of the Department for Digital, Culture, Media and Sport from the NSC is also puzzling given the criticality of its work on developing skills to the successful delivery of the 2016 NCSS.[246] Having stated earlier that operators must assume greater responsibility for cyber resilience at board level, with a clear point of accountability (paragraphs 67–69), we note that the Government is failing to do the same at the equivalent management level.

79. **Focused and proactive political leadership from the centre of Government is essential in driving change and ensuring a consistent approach across the many departments and agencies with responsibility for the resilience of CNI to cyber threats. We are concerned that the current complex arrangements for ministerial responsibility mean that day-to-day oversight of cross-government efforts is, in reality, led by officials, with Ministers only occasionally 'checking in'. This is wholly inadequate to the scale of the task facing the Government, and inappropriate in view of the Government's own assessment that major cyber attacks are a top-tier national security threat.**

80. ***There should be a Cabinet Office Minister designated as cyber security lead who, as in a war situation, has the exclusive task of assembling the resources—in both the public and private sectors—and executing the measures needed to defend against the threat. This Minister should therefore be responsible and accountable for the cross-government development and delivery of the National Cyber Security Strategy and Programme, including those elements relating to CNI. This Minister should therefore:***

- ***be empowered to hold departmental Ministers to account;***
- ***sit on the National Security Council (NSC) and relevant NSC sub-committees; and***
- ***oversee the work of the National Cyber Security Centre and the relevant section of the National Security Secretariat.***

81. ***The Government should also provide our Committee with evidence of the NSC sub-committees' active oversight of cross-government efforts to improve the cyber resilience of the UK's CNI. Its recent decision to share summaries of the agendas for relevant NSC sub-committees with us, in confidence and on a regular basis, is a welcome starting point.***

Technical leadership: the National Cyber Security Centre

82. The creation of the NCSC, as the UK's technical (rather than strategy or policy) lead on cyber security, was the 'cornerstone' of the 2016 NCSS. It makes a major contribution to, and frequently leads on, the initiatives described in the 2016 Strategy. In relation to CNI in particular, it has provided threat intelligence, technical guidance—especially in implementing the NIS Regulations (see Chapter 4)—and incident response support to lead Government departments, CNI operators and regulators. It has also taken the technical

[246] In addition to work on cyber security skills, DCMS also delivers work on implementing the GDPR and NIS Regulations, on the security of consumer Internet of Things devices and on programmes aimed at growing the cyber security industry in the UK. DCMS, "Cyber Security Month", 31 October 2018, accessed 13 November 2018

lead on efforts to make future CNI, such as 5G mobile internet, 'secure by design',[247] guided research in areas relevant to the resilience of CNI, and supported initiatives intended to develop the range of technical and specialist skills needed by CNI operators and regulators.[248]

Providing a single point of contact

83. The evidence shows that the NCSC has had a positive impact in the two years since it was established in October 2016. We heard that the NCSC's creation had, by and large, achieved the Government's stated aim of rationalising the many Government bodies that previously dealt with elements of cyber security policy,[249] [250] although there continues to be some confusion about the relationship between the NCSC and the Centre for the Protection of National Infrastructure (the Government authority for protective security advice).[251] However, echoing our own concerns about a strategic and policy vacuum at the centre of Government (above), the Information Assurance Advisory Council—a not-for-profit research organisation—also suggested that cross-government leadership on policy has become less clear since the NCSC was established. They told us:

> the cross Whitehall function seems to have taken a retrograde step with the effective loss of the original focal point for coordination—the Office of Cyber Security and Information Assurance (OCSIA). It is currently unclear who leads, who coordinates and who is responsible, including at ministerial level, with activities and policy seemingly diffuse and ambiguous across departments.[252]

Collaborating with the private sector

84. We heard that, despite reports of early tensions, the NCSC is making progress on developing collaborative relationships with private-sector CNI operators and regulators.[253] This is essential, not only because of the particular need for an effective public-private relationship in ensuring the resilience of the UK's CNI, but also because the NCSC does not have enforcement powers, even in relation to the NIS Regulations.[254] Witnesses brought to our attention two key points on which they felt the NCSC could improve:

[247] NCSC, "Annual Review 2018", October 2018, pp. 30–33

[248] Joint Committee on the National Security Strategy, Second Report of 2017–19, *Cyber Security Skills and the UK's Critical National Infrastructure*, HL Paper 172, HC 706; NCSC, "Annual Review 2018", October 2018, pp. 40–45; Imperial College London (CNI0009) para 10

[249] Q16; Q36 [Lyndon Nelson, Paul Smith]; Nettitude (CNI0003) para 15; Jamie Collier (CNI0006) paras 3.3, 7; Palo Alto Networks (CNI0011) para 12; Chatham House (CNI0012) para 2.1; techUK (CNI0015) paras 7, 36–37; BT Group (CNI0018) para 5.2; Aerospace, Defence, Security & Space (CNI0020) paras 1.12–1.13; Nokia (CNI0022) para 5.2; Corero (CNI0023) para 16

[250] These bodies included the CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and relevant parts of the CPNI. NCSC, "About us", accessed 31 October 2018; HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, p. 29

[251] UK Computing Research Committee, UKCRC (CNI0005) paras 14–16. Professor Chris Johnson, writing on behalf of UK CRC, also stated his concern that the function previously performed by CERT UK has been given much less emphasis since it was incorporated into the NCSC. UK Computing Research Committee, UKCRC (CNI0005) para 16

[252] Information Assurance Advisory Council (CYB0008) para 4. While the NCSC does not lead the development of cyber security strategy, it does have input into the strategy-making process, via the NSC. Q60 [Ciaran Martin]

[253] Q16; Q36 [Lyndon Nelson, Paul Smith]; Palo Alto Networks (CNI0011) para 12; techUK (CNI0015) paras 36, 39; Aerospace, Defence, Security & Space (CNI0020) para 1.12; Nokia (CNI0022) para 5.2

[254] Intelligence and Security Committee of Parliament, *Annual Report 2016–2017*, HC 655, paras 98–101

- its geographical reach beyond London.[255] The NCSC's 2018 Annual Review states its intention to expand its "footprint geographically";[256] and

- the extent and speed of its intelligence-sharing.[257] The NCSC is uniquely positioned—as a part of GCHQ—to provide the type and level of intelligence (meaning, in this instance, analysed information based on classified intelligence) that CNI operators and regulators need to manage operational cyber risk effectively.[258] But Paul Smith of the trade body Water UK told us that the water sector does not even have enough information to understand why the Government classifies it as a "low threat" sector,[259] while the Financial Conduct Authority—the financial regulatory authority—suggested that the Government tends to "overclassify" information. It said that the Government can be too slow in releasing information that may "help prevent significant harm from occurring".[260]

85. There are other fundamental questions about the NCSC's status as part of GCHQ. On the one hand, this arrangement confers a notable advantage, as the NCSC has easy access to key expertise and up-to-date intelligence. On the other hand, and as Emily Taylor, an Associate Fellow at Chatham House, explained, there is an inherent tension between the main function of GCHQ (gathering intelligence on threats, and keeping it private) and that of the NCSC (using a sanitised version of that intelligence to help operators and regulators defend CNI against those threats).[261] We note that the 2004 Butler Report cautioned against intelligence and policy implementation becoming too closely intertwined, as a matter of principle.[262] In discussing his experience of the response to the WannaCry attack, NHS Digital's Rob Shaw raised his concerns about how this apparent conflict of interest on the part of the NCSC has been manifested in practice. He said:

> There will be times when the NCSC has to take a security view on something and we have to take a healthcare view on it, so I have to have a difficult discussion. … If there was a security issue, I could not, for example, do anything that meant a risk to patient safety. I would always have to make sure that I put patient safety before intelligence.[263]

[255] Manchester Metropolitan University (CNI0001) para 4.6; UK Computing Research Committee, UKCRC (CNI0005) para 14. The UK Computing Research Committee stated that direct contact between the NCSC and CNI operators declines rapidly outside the home counties.

[256] NCSC, "Annual Review 2018", October 2018, p. 11

[257] Professor Chris Johnson, on behalf of the UK Computing Research Committee, suggested that information-sharing between the NCSC and industry was "one-way; from industry into the NCSC". UK Computing Research Committee, UKCRC (CNI0005) para 12
ADS said that "clearer communication on the part of Government to industry around the risks facing individual business sectors would help to encourage an even stronger response in industry". Aerospace, Defence, Security and Space (CNI0020) para 1.12

[258] Q8 [Phil Sheppard]

[259] Q36 [Paul Smith]

[260] Financial Conduct Authority (CNI0033) para 12.1

[261] Emily Taylor recommended that the NCSC be formally separated from GCHQ. Emily Taylor, Chatham House (CNI0012) paras 3.5–3.8. See also UK Computing Research Committee, UKCRC (CNI0005) para 12; Royal Society (CYB0040) para 3

[262] *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Counsellors*, HC 898, July 2004, paras 33–36

[263] Q16 [Rob Shaw]

Meeting demand for NCSC services and expertise

86. There is an issue about whether the NCSC has sufficient capacity to meet the considerable—and growing—demand on its services and expertise.[264] It is a relatively new organisation, whose influence has grown quickly since it was established in October 2016. Ciaran Martin told us that the NCSC has 740 staff and a budget of £285 million for the 2016–2021 period, which provides financial and strategic stability (paragraph 77).[265]

87. However, the NCSC's remit is also already considerable. In the past year, it has reportedly "worked with thousands of systems and hundreds of organisations across the UK" in relation to CNI.[266] Its work in support of the UK's CNI is just one of its main responsibilities, which also includes engaging with the wider economy, including small and medium-sized enterprises, and raising public awareness on cyber security.[267] Furthermore, the evidence we have received on CNI suggests that expectations—at least on the part of CNI operators and regulators, and even of other parts of Government—already exceed the NCSC's capacity (for example, as was discussed in Chapter 4 in relation to the implementation of the NIS Regulations). NHS Digital's Rob Shaw also raised this issue in relation to incident response—a key element of the NCSC's work. Describing his experience of the WannaCry attack in May 2017, he told us that

> I expected an army of NCSC staff to appear on the hillside and come in to help us out, but it said, "Where do you want either of our staff?" It does not have a lot of people with the expertise to do things on the ground.[268]

88. As we noted in our July Report on cyber security skills,[269] this situation is compounded by what Ciaran Martin described as the "constant and difficult challenge" of recruiting the deep technical expertise it needs in areas such as 5G mobile internet.[270] Although the NCSC supplements its workforce with secondees from the private sector under the Industry 100 initiative,[271] its sector-specific expertise remains limited; for example, Professor Chris Johnson, of the UK Computing Research Committee, reported that there are still only "3 or 4 individuals" in the NCSC with "significant expertise" in aviation.[272] There is a risk that such capacity constraints will undermine the NCSC in its role as the UK's 'one-stop shop' for technical advice and support, and therefore its ability to support the delivery of the 2016 NCSS. Several witnesses called on the Government to support the NCSC's further development, through additional funding if necessary.[273]

[264] Qq26–28. For example, Ofgem's Jonathan Brearley told us that the energy sector is "heavily reliant" on the NCSC and stated Ofgem's intention to rely further on the NCSC in its new capacity as Competent Authority. Qq26, 36 [Jonathan Brearley]

[265] Ciaran Martin explained that this total number can be broken down into three sections of approximately 250, with the first group working on the "deeply operational" aspect of the NCSC and GCHQ's work, the second on "understanding technology and how to protect it", and the third as "outward-facing advisers, communications specialists and so on", including "a couple of dozen public communications specialists". Qq56, 61 [Ciaran Martin]

[266] NCSC, "Annual Review 2018", October 2018, p. 30

[267] NCSC, "Annual Review 2018", October 2018

[268] Q16 [Rob Shaw]

[269] Joint Committee on the National Security Strategy, Second Report of 2017–19, *Cyber Security Skills and the UK's Critical National Infrastructure*, HL Paper 172, HC 706, para 9

[270] Q61 [Ciaran Martin]

[271] Ciaran Martin told us that, in June 2018, there were 80 such private-sector experts working for the NCSC, although not all of them worked full time. Q61 [Ciaran Martin]; NCSC, "Introduction to Industry 100", accessed 31 October 2018

[272] UK Computing Research Committee (CNI0005) para 10

[273] Jamie Collier (CNI0006) para 3.3; UK Computing Research Committee, UKCRC (CNI0005) para 11; Palo Alto Networks (CNI0011) paras 14, 17; Corero (CNI0023) para 16

89. **The National Cyber Security Centre has had an impressive impact in the two years since it was established as the national technical authority on cyber security. Although there are areas for improvement, it has made important contributions across a variety of Government and industry initiatives in relation to CNI, despite its lack of enforcement powers. However, we heard there are unresolved tensions derived from its status as part of GCHQ—an institutional relationship that also provides significant advantages. It is also essential that the NCSC's proactive leadership on the technical aspects of the cyber resilience of CNI is not treated by Ministers as a substitute for strong political leadership in driving change across CNI sectors and relevant departments.**

90. **We continue to have concerns about the capacity of the NCSC to meet growing demand for its services and expertise. As the Government's 'one-stop shop' for technical advice, the NCSC is integral to the Government's and private sector's efforts to improve the resilience of the UK's CNI to cyber attack. However, its effectiveness will be limited unless it has access to the experts it needs in the numbers it requires. Consideration must also be given to likely future demands on the NCSC's resources as technology continues to advance and the threat continues to grow.**

91. ***The Government should publish a plan for the institutional development of the NCSC over the next decade, taking account of anticipated technological progress and setting out the resources and range of skills and expertise that the NCSC is likely to need. These requirements should be addressed in the Government's forthcoming cyber security skills strategy. Its budget—currently running to 2020–21—should be extended beyond that time horizon in next year's Spending Review as a ring-fenced fund separate from (and safe from) general departmental budget pressures.***

Conclusions and recommendations

Protecting CNI against cyber attack: a 'wicked' problem

1. The cyber threat to the UK's CNI is growing. It is also evolving: hostile states are becoming more aggressive in their behaviour, with some states—especially Russia—starting to explore ways of disrupting CNI, in addition to conducting espionage and theft of intellectual property. Furthermore, while states still represent the most acute and direct cyber threat, non-state actors such as organised crime groups are developing increasingly sophisticated capabilities. (Paragraph 18)

2. Fast-changing threats and the rapid emergence of new vulnerabilities make it impossible to secure CNI networks and systems completely. Continually updated plans for improving CNI defences and reducing the potential impact of attacks must therefore be the 'new normal' if the Government and operators are to be agile in responding to this changing environment and in taking advantage of constant technological innovation. Building the resilience of CNI to cyber attacks in this way will make it harder for an attacker to achieve their objective—whoever that attacker may be, whatever their motive and however they choose to attack. (Paragraph 19)

Defining 'critical' national infrastructure

3. 'Critical' national infrastructure is, by definition, a priority for the Government and industry. However, as the economy becomes more interconnected, it is increasingly difficult to determine which elements are truly critical. The 2016 National Cyber Security Strategy provides few clues as to how the Government is managing this issue or how it is prioritising its efforts between CNI sectors. It also fails to acknowledge the varying complexity of the CNI sectors and the bearing this should have on the Government's approach. Asserting that the UK is at the forefront of international efforts on cyber security is not sufficient. (Paragraph 26)

4. *The next National Cyber Security Strategy, due for publication in 2021 should be informed by a mapping of the key interdependencies between CNI sectors—and therefore of national-level cyber risk to CNI—which the Government should complete as soon as possible and keep under continual review. The priorities identified in the next Strategy should also take account of the CNI sectors' respective maturity in terms of cyber resilience and the varying levels of Government influence over operators in each sector.* (Paragraph 27)

Setting and delivering strategic objectives, and measuring progress

5. The 2016 National Cyber Security Strategy states that ensuring the resilience of the UK's critical national infrastructure to cyber attack is a priority for the Government. But the Strategy does not set out (a) what specifically the Government wants to achieve; (b) over what timeframe; or (c) how it intends to measure progress. We are therefore concerned that despite the designation of major cyber attacks as a top-tier threat to UK national security, the Government does not have clearly defined

objectives for the five-year period covered by the Strategy nor a structured plan for delivering them. This echoes our findings specifically in relation to cyber security skills, which we set out in our July Report. (Paragraph 34)

6. The Government is unwilling to publish any information about the 2016–2021 National Cyber Security Programme other than its total budget of £1.9 billion. While we accept that some elements of the NCSP are security-sensitive and therefore should not be made public, such lack of transparency about such large sums of public money is of serious concern. It is also a backwards step, given that the previous Government published Annual Reports and high-level budget breakdowns by activity for the earlier 2011–2016 NCSP. (Paragraph 35)

7. *The Government should resume publishing Annual Reports for the National Cyber Security Programme to improve transparency and aid external scrutiny. These should set out progress made, the challenges faced, and a breakdown of the budget by type of activity and by department or agency; it would also present a regular opportunity to review and adjust plans in response to changing threats, vulnerabilities and technological innovation (as we concluded in paragraph 19). Given the relatively large sum of public money and the many departments and agencies involved, the Government should also support a programme-wide audit of the NCSP by the National Audit Office to provide public and Parliamentary assurance.* (Paragraph 36)

An "expanded role" for the Government on CNI?

8. The Government's current approach to improving the cyber resilience of the UK's critical national infrastructure is long on aspiration but short on delivery. Establishing the National Cyber Security Centre as the national technical authority and introducing more robust regulation for some CNI sectors were both important steps. The latter was mandatory for the UK as an EU member state, however. It appears that the Government is reluctant to move more forcefully and, by default, continues to rely on market forces to improve operators' cyber resilience, despite recognising the previous failure of this approach. Its efforts so far certainly fail to do justice to the status of major cyber attacks as a top-tier threat to national security or to the importance of CNI to the economy. Greater urgency is required if the UK is to 'get ahead' and 'stay ahead' of the cyber threats to its CNI. (Paragraph 43)

9. *As we concluded in relation to cyber security skills in our July Report, the Government must first understand the problem before it can address it. The Government should therefore immediately commission work to understand how and why the market has failed to deliver improved cyber resilience of CNI in both the public and private sectors. Only then will it be in a position to identify the targeted interventions and incentives—whether regulatory or otherwise—that will drive up cyber resilience of CNI, while also establishing the culture and practices necessary for continual improvement in the long term.* (Paragraph 44)

Regulation: fixing market failure by setting a higher benchmark

10. The Network and Information Systems Regulations offer a more robust regulatory framework for many CNI sectors, especially in making it mandatory for operators to report incidents where their impact exceeds a predetermined threshold. Although these regulations have only recently come into force, we expect them to set a higher benchmark for cyber risk management in those CNI sectors where they apply. They should also, we hope, foster a culture of proactive and continual risk management by CNI operators, moving away from a 'tick-box compliance' approach. (Paragraph 51)

11. Nevertheless, the NIS Regulations are not a 'silver bullet':

- the NIS Regulations are limited in scope, leaving some CNI sectors still without statutory regulation and enforcement powers for cyber risk management;
- the fragmented responsibility for the NIS Regulations' implementation across Whitehall, Devolved Administrations and regulators remains confusing and acts as a barrier to cross-sector consistency and collaboration—in particular, the introduction of joint Competent Authorities in some sectors clouds accountability and effectiveness; and
- some designated 'Competent Authorities' currently lack the expertise and capacity to provide credible assurance of operators' efforts—an issue we addressed directly in our July Report on cyber security skills.

We are therefore concerned that the NIS Regulations will not be enough in themselves to achieve the required leap forward in cyber resilience across all CNI sectors (Paragraph 52)

12. Threat- and intelligence-led penetration testing shows promise as a mechanism for providing technical assurance of CNI operators' cyber risk management—all the more important in the absence of agreed metrics for cyber risk and resilience. However, such testing should be used in combination with other methods of regulatory assurance because it only provides a snapshot of operational resilience at a particular moment in time against a particular set of threats. (Paragraph 56)

13. *The Government should establish a plan (a) for the development of threat- and intelligence-led penetration testing and its roll-out across all CNI sectors that takes account of the mixed maturity of the sectors in terms of their cyber resilience; (b) for the development of the test methodology; and (c) for developing the cyber security industry's capacity to deliver such advanced and accredited testing at scale. It should address the last point in its forthcoming cyber security skills strategy which, as we urged in our July Report, should be published as a matter of priority.* (Paragraph 57)

14. The NIS Regulations will continue to apply in the UK following Brexit. However, the mechanism for UK participation in EU-wide information-sharing and capacity-building is still subject to negotiation. *Given that cyber threats do not stop at national borders, the Government should prioritise maintaining access to the EU's NIS Coordination Group and its workstreams to facilitate continued information-sharing and collaboration with EU Member States.* (Paragraph 60)

Cultural change: creating an environment for continual improvement

15. *The Government should set out in its response to this Report its assessment of how, and how effectively, the Huawei Cyber Security Evaluation Centre Oversight Board provides additional assurance in relation to the UK's cyber security.* (Paragraph 66)

16. A more holistic and effective approach to strengthening the cyber resilience of CNI requires changing the culture of CNI operators and their extended supply chains. Embedding the view that cyber risk is another business risk, which must be proactively managed, will be central to this process. It is especially important for those private-sector operators whose commercial interests may not always align with the demands of national security. (Paragraph 73)

17. *The Government should give urgent consideration to non-regulatory incentives and interventions that have the potential to drive cultural change across CNI sectors, establishing an environment in which continual improvement is encouraged. The issues it should consider include:*

- *how managing cyber risk through and within the extended supply chains of CNI operators could be encouraged;*

- *how the Government can best support operators in managing cyber risk associated with hardware, software and services bought 'off the shelf', especially those procured from major international suppliers;*

- *improving board-level expertise and accountability. This includes identifying an expert board member with specific responsibility for cyber resilience and mandatory corporate reporting on cyber resilience, in accordance with the spirit of forthcoming reforms to the Companies Act 2006; and*

- *how cyber insurance might be used to improve operators' cyber practices, and how the Government can support the market in maturing more quickly.* (Paragraph 74)

Political leadership: driving change across Government and CNI sectors

18. Focused and proactive political leadership from the centre of Government is essential in driving change and ensuring a consistent approach across the many departments and agencies with responsibility for the resilience of CNI to cyber threats. We are concerned that the current complex arrangements for ministerial responsibility mean that day-to-day oversight of cross-government efforts is, in reality, led by officials, with Ministers only occasionally 'checking in'. This is wholly inadequate to the scale of the task facing the Government, and inappropriate in view of the Government's own assessment that major cyber attacks are a top-tier national security threat. (Paragraph 79)

19. *There should be a Cabinet Office Minister designated as cyber security lead who, as in a war situation, has the exclusive task of assembling the resources—in both the public and private sectors—and executing the measures needed to defend against the threat. This Minister should therefore be responsible and accountable for the cross-government development and delivery of the National Cyber Security Strategy and Programme, including those elements relating to CNI. This Minister should therefore:*

- *be empowered to hold departmental Ministers to account;*
- *sit on the National Security Council (NSC) and relevant NSC sub-committees; and*
- *oversee the work of the National Cyber Security Centre and the relevant section of the National Security Secretariat.* (Paragraph 80)

20. *The Government should also provide our Committee with evidence of the NSC sub-committees' active oversight of cross-government efforts to improve the cyber resilience of the UK's CNI. Its recent decision to share summaries of the agendas for relevant NSC sub-committees with us, in confidence and on a regular basis, is a welcome starting point.* (Paragraph 81)

21. The National Cyber Security Centre has had an impressive impact in the two years since it was established as the national technical authority on cyber security. Although there are areas for improvement, it has made important contributions across a variety of Government and industry initiatives in relation to CNI, despite its lack of enforcement powers. However, we heard there are unresolved tensions derived from its status as part of GCHQ—an institutional relationship that also provides significant advantages. It is also essential that the NCSC's proactive leadership on the technical aspects of the cyber resilience of CNI is not treated by Ministers as a substitute for strong political leadership in driving change across CNI sectors and relevant departments. (Paragraph 89)

22. We continue to have concerns about the capacity of the NCSC to meet growing demand for its services and expertise. As the Government's 'one-stop shop' for technical advice, the NCSC is integral to the Government's and private sector's efforts to improve the resilience of the UK's CNI to cyber attack. However, its effectiveness will be limited unless it has access to the experts it needs in the numbers it requires. Consideration must also be given to likely future demands on the NCSC's resources as technology continues to advance and the threat continues to grow. (Paragraph 90)

23. *The Government should publish a plan for the institutional development of the NCSC over the next decade, taking account of anticipated technological progress and setting out the resources and range of skills and expertise that the NCSC is likely to need. These requirements should be addressed in the Government's forthcoming cyber security skills strategy. Its budget—currently running to 2020–21—should be extended beyond that time horizon in next year's Spending Review as a ring-fenced fund separate from (and safe from) general departmental budget pressures.* (Paragraph 91)

Annex 1: Glossary

ABI—Association of British Insurers

ACD—Active Cyber Defence

CiSP—Cyber Security Information Sharing Platform

CNI—Critical national infrastructure

CSIRT—Computer Security Incident Response Team

DHS—Department for Homeland Security

GDPR—General Data Protection Regulation

ICO—Information Commissioner’s Office

IISS—International Institute for Strategic Studies

NCSC—National Cyber Security Centre

NCSP—National Cyber Security Programme

NCSS—National Cyber Security Strategy

NIS Directive—Network and Information Systems Directive

NSC—National Security Council

NSC (SDSR)—National Security Council sub-committee on the Strategic Defence and Security Review

NSC (THRC)—National Security Council sub-committee on Threats, Hazards, Resilience and Contingencies

NSS & SDSR—National Security Strategy and Strategic Defence and Security Review

ONR—Office for Nuclear Regulation

OT—Operational technology

Annex 2: Joint Committee on the National Security Strategy

The Members of the Joint Committee that conducted the inquiry were

- Margaret Beckett MP (Chair)
- Lord Brennan
- Lord Campbell of Pittenweem
- Yvette Cooper MP
- James Gray MP
- Mr Dominic Grieve MP
- Lord Hamilton of Epsom
- Lord Harris of Haringey
- Baroness Healy of Primrose Hill
- Baroness Henig
- Dan Jarvis MP
- Lord King of Bridgewater
- Baroness Lane-Fox of Soho
- Dr Julian Lewis MP
- Angus Brendan MacNeil MP
- Robert Neill MP
- Lord Powell of Bayswater
- Rachel Reeves MP
- Lord Trimble
- Tom Tugendhat MP
- Stephen Twigg MP
- Theresa Villiers MP

Declarations of interests (Lords)[274]

The following interests, relevant to this inquiry, were declared:

Lord Brennan

- *Member, Advisory Board of Assured Enterprises Inc, an American IT security company based in Virginia, USA*

Lord Harris of Haringey

- *Non-executive Director, Cyber Security Challenge UK Ltd*
- *UK Co-ordinator, Electric Infrastructure Security Council*
- *Chair, Independent Reference Group, National Crime Agency*

Baroness Lane-Fox of Soho

- *Director of the Board of Twitter (paid) since May 2016*
- *Chancellor, Open University*

Lord Powell of Bayswater

- *Member of the Advisory Board of Thales UK*

A full list of Committee Members' interests can be found in the Register of Lords' Interests: https://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests/ and in the House of Commons Register of Members' Financial Interests: http://www.publications.parliament.uk/pa/cm/cmregmem/contents.htm

[274] The declarations of interests by the Commons Members are available in the Committee's Formal Minutes 2017–19.

Formal minutes

Monday 12 November 2018

Members present:

Margaret Beckett MP, in the Chair

Lord Brennan
Lord Campbell of Pittenweem
James Gray MP
Mr Dominic Grieve MP
Lord Hamilton of Epsom
Lord Harris of Haringey
Baroness Healy of Primrose Hill
Lord King of Bridgwater
Dr Julian Lewis MP
Lord Trimble
Theresa Villiers MP

Draft Report, *Cyber Security of the UK's Critical National Infrastructure,* proposed by the Chair, brought up and read.

Ordered, That the draft Report be considered, paragraph by paragraph.

Paragraphs 1 to 91 agreed to.

Annexes agreed to.

Summary agreed to.

Resolved, That the Report be the Third Report of the Committee.

Resolved, That the Chair make the Report to the House of Commons and that the Report be made to the House of Lords.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of House of Commons Standing Order No. 134.

[Adjourned to 19 November at 4.00pm

Witnesses

The following oral evidence was received in the last Parliament by the previous Committee for their inquiry into *Cyber Security: UK National Security in a Digital World*, and can be viewed on the inquiry publications page of the Committee's website.

Monday 27 March 2017

Question number

Dr Richard Horne, Cyber Security Partner, PricewaterhouseCoopers, **Rowland Johnson**, CEO, Nettitude, **Dr Brandon Valeriano**, Reader in Law and Politics, Cardiff University, **Ollie Whitehouse**, Technical Director, NCC Group Q1–16

The following witnesses gave evidence in the 2017–19 Parliamentary session for the inquiry into *Cyber Security of the UK's Critical National Infrastructure*. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Monday 12 March 2018

Question number

Phil Sheppard, Director, Gas Transmission Owner, National Grid, **Peter Gibbons**, Chief Security Officer, Network Rail and **Rob Shaw**, Deputy CEO, NHS Digital Q1–25

Monday 23 April 2018

Paul Smith, Strategic Security Board, Water UK, **Lyndon Nelson**, Deputy Chief Executive and Executive Director for Supervisory Risk Specialists and Regulatory Operations, Prudential Regulation Authority, **Jonathan Brearley**, Executive Director for Systems and Networks, Ofgem and **Steve Unger**, Chief Technology Officer, Ofcom Q26–38

Monday 21 May 2018

Rob Crook, Managing Director of Cyber Security and Intelligence, Raytheon UK, **Dr Alastair MacWillson**, Chair of Institute of Information Security Professionals and Chair of Qufaro at Bletchley Park, **Elliot Rose**, Digital Trust Cyber and Security, PA Consulting Group and **Ruth Davis**, Head of Commercial Strategy and Public Policy, BT Security Q39–53

Monday 25 June 2018

Rt Hon David Lidington MP, Chancellor of the Duchy of Lancaster and **Ciaran Martin**, Chief Executive Officer, National Cyber Security Centre Q54–63

Published written evidence

The following written evidence was received in the last Parliament by the previous Committee for their inquiry into *Cyber Security: UK National Security in a Digital World*, and can be viewed on the inquiry publications page of the Committee's website.

CYB numbers are generated by the evidence processing system and so may not be complete.

1 ADS Group (CYB0023)

2 Altran UK (CYB0043)

3 Association of British Insurers (CYB0019)

4 Brandon Valeriano (CYB0045)

5 British Retail Consortium (CYB0022)

6 British Standards Institution (CYB0006)

7 BT (CYB0025)

8 Cabinet Office (CYB0020)

9 Cifas (CYB0035)

10 Corsham Institute (CYB0011)

11 Dr Tara McCormack (CYB0042)

12 EMEA (CYB0041)

13 Federation of Small Businesses (CYB0031)

14 Foundation for Information Policy Research (CYB0034)

15 Fujitsu (CYB0036)

16 Information Assurance Advisory Council (CYB0008)

17 Institution of Engineering and Technology (CYB0037)

18 International Centre for Security Analysis, King's College London (CYB0004)

19 ISACA (CYB0024)

20 ITSPA (CYB0033)

21 Mayor's Office for Policing And Crime (CYB0030)

22 Microsoft (CYB0028)

23 Mr Andreas Haggman (CYB0017)

24 Mr Pete Cooper (CYB0013)

25 Mr Stuart Hyde (CYB0012)

26 NCC Group (CYB0014)

27 Ollie Whitehouse (CYB0044)

28 PA Consulting Group (CYB0009)

29 Palo Alto Networks (CYB0026)

30 Pinsent Masons LLP (CYB0016)

31 PricewaterhouseCoopers (CYB0003)

32 Privacy International (CYB0005)

33 Professor Martyn Thomas (CYB0032)

34 Rowland Johnson (CYB0046)

35 RUSI (CYB0039)

36 techUK (CYB0021)

37 The Information Commissioner's Office (CYB0038)

38 The Royal Society (CYB0040)

39 Trustonic (CYB0027)

40 UKCloud & The Corsham Institute (CYB0002)

41 Yorkshire Cyber Security Cluster (CYB0015)

The following written evidence was received in the 2017–19 Parliamentary session for the inquiry into *Cyber Security of the UK's Critical National Infrastructure*, and can be viewed on the inquiry publications page of the Committee's website.

CNI numbers are generated by the evidence processing system and so may not be complete.

1 ABI (CNI0026)

2 Aerospace, Defence, Security & Space (CNI0020)

3 Altran UK (CNI0008)

4 BT Group (CNI0018)

5 Cabinet Office NSS (CNI0030)

6 Cabinet Office, National Security Secretariat (CNI0013)

7 Cambridge Centre for Risk Studies (CNI0025)

8 Chatham House (CNI0012)

9 Cisco (CNI0016)

10 Corero (CNI0023)

11 CREST (CNI0028)

12 CrowdStrike (CNI0014)

13 CyLon (CNI0032)

14 Dr Martyn Thomas (CNI0004)

15 Financial Conduct Authority (CNI0033)

16 Glasswall Solutions Limited (CNI0007)

17 Imperial College London (CNI0009)

18 ISACA (CNI0010)

19 Jamie Collier (CNI0006)

20 Lloyd's (CNI0034)

21 Manchester Metropolitan University (CNI0001)

22 NCC Group (CNI0002)

23 Nettitude (CNI0003)

24 Nokia (CNI0022)

25 Office for Nuclear Regulation (CNI0031)

26 PA Consulting (CNI0029)

27 Palo Alto Networks (CNI0011)

28 Pete Cooper (CNI0019)

29 Red Hat Inc (CNI0021)

30 techUK (CNI0015)

31 The International Institute for Strategic Studies (CNI0017)

32 UK Computing Research Committee, UKCRC (CNI0005)

33 UKCloud Ltd (CNI0024)

34 Water UK (CNI0027)

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee’s website. The reference number of the Government’s response to each Report is printed in brackets after the HC printing number.

Session 2017–19

First Report	National Security Capability Review: A changing security environment	HL Paper 104 HC 759
Second Report	Cyber Security Skills and the UK’s Critical National Infrastructure	HL Paper 172 HC 706
First Special Report	National Security Capability Review: A changing security environment: Government Response to the Committee’s First Report of Session 2017–19	HL Paper 197 HC 1646
Second Special Report	Cyber Security Skills and the UK’s Critical National Infrastructure: Government Response to the Committee’s Second Report of Session 2017–19	HL Paper 198 HC 1658