House of Commons
House of Lords

Joint Committee on the
National Security Strategy

A hostage to fortune: ransomware and UK national security

First Report of Session 2023–24

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 4 December 2023

Ordered by the House of Lords to be printed 4 December 2023

HC 194
HL Paper 23
Published on 13 December 2023
by authority of the House of Commons
and the House of Lords

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 Butler of Brockwell (*Crossbench*)

Baroness Crawley (*Labour*)

Lord Dannatt (*Crossbench*)

Baroness Fall *(Conservative)*

Lord Reid of Cardowan *(Labour)*

Lord Robathan *(Conservative)*

Lord Sarfraz *(Conservative)*

Lord Snape *(Labour*)

Viscount Stansgate (*Labour*)

Lord Strasburger *(Liberal Democrat)*

House of Commons

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

Sarah Champion MP (*Labour, Rotherham*)

Robert Courts MP (*Conservative, Witney*)

Richard Graham MP (*Conservative, Gloucester*)

Diana Johnson MP (*Labour, Kingston upon Hull North*)

Darren Jones MP (*Labour, Bristol North West*)

Alicia Kearns MP (*Conservative, Rutland and Melton*)

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

Stephen McPartland MP (*Conservative, Stevenage*)

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

Bob Stewart MP (*Conservative, Beckenham*)

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

After his appointment to a Ministerial post on 6 September 2022, Tom Tugendhat MP recused himself from meetings and ceased to receive Committee papers.

After his appointment to a Shadow Ministerial post on 4 September 2023, Darren Jones MP also recused himself from meetings and ceased to receive Committee papers.

Lord Ashton of Hyde was a JCNSS Member from January 2023 until June 2023.

Mr Tobias Ellwood was a JCNSS Member until 11 November 2023, when he was discharged from the Committee.

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 Chair.

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.

Committee staff

The current staff of the Committee are Grace Annan (Commons Committee Specialist), Lucy Arora (Head of International Affairs Unit), Medha Bhasin (Commons Clerk of the Committee), Carolyn Bowes (Commons Committee Operations Officer), Jessica Bridges Palmer (Senior Media and Communications Officer), Glenn Chapman (Lords Committee Operations Officer), Eleanor Ferguson (Committee Specialist, International Affairs Unit), Ashlee Godwin (Commons Head of International Affairs and National Security Hub) and Beth Hooper (Lords Clerk).

Harriet Deane (Commons Clerk of the Committee) throughout this inquiry and is now on maternity leave.

Contact

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 numbers for enquiries are 020 7219 3869/4043; the Committee's email address is jcnss@parliament.uk

Contents

Summary

Ransomware is a form of malware designed to damage and destroy computers and computer systems, usually to facilitate extortion. It is also increasingly linked to data theft, and to threats to publish sensitive information online. Mass data loss from an attack can be irreversible, even when the ransom is paid. Due to its potential ability to bring the UK to a standstill, ransomware has been identified by UK authorities as the number one cyber threat to the nation.

Having ‘exploded’ in 2021, the ransomware threat is still as severe as it has ever been, and the UK is one of the most targeted countries in the world. A mature and complex ecosystem has evolved, involving an increasingly sophisticated threat actor; ransomware is also now marketed as a service, which can be purchased by the uninvolved e.g. criminal gangs, making it more widely available to those who wish to inflict harm for profit. Past attacks have shown that ransomware can cause severe disruption to the delivery of core Government services, including healthcare and child protection, as well as ongoing economic losses.

The majority of ransomware attacks against the UK are from Russian-speaking perpetrators, and the Russian Government’s tacit (or even explicit) approval of this activity is consistent with the Kremlin’s disruptive, zero-sum-game approach to the West. This is not a straightforward state threat, however. For many Russian hackers, ransomware is simply an easy way to make large sums of money, with next-to-no chance of being caught or prosecuted.

The Government and the National Cyber Security Centre (NCSC) have focused their counter-ransomware efforts predominantly on resilience. Nevertheless, large swathes of UK critical national infrastructure (CNI) remain vulnerable to ransomware, particularly in sectors still relying on legacy IT systems, and we have particular concerns about cash-strapped sectors such as health and local government. Supply chains are also particularly vulnerable and have been described by the NCA as the ‘soft underbelly’ of CNI.

As a result of these vulnerabilities, a coordinated and targeted attack has the potential to take down large parts of UK CNI and public services, causing severe damage to the economy and to everyday life in the UK. Given the poor implementation of existing cyber resilience regulations, the Government should scope the feasibility of establishing a cross-sector regulator on CNI cyber resilience. As part of the National Exercise Programme, it should also hold regular national exercises to prepare for the impact of a major national ransomware attack affecting multiple CNI sectors, engaging CNI operators to stress-test their response and ensure a swift recovery. In addition, the NCSC should be funded to establish an enhanced and dedicated local authority resilience programme, including intensive support for local exercising and on securing council supply chains.

The impact of a ransomware attack on its victims is significant, with many organisations taking months to recover. Despite this, most victims currently receive next-to-no support from law enforcement or Government agencies. The NCSC and National Crime Agency (NCA) should be funded to provide support to all public sector victims

of ransomware, to the point of full recovery. Cyber insurance can also be a vital source of support, but there remains a woeful lack of coverage. The Government should work with the insurance sector to establish a re-insurance scheme for major cyber-attacks, to ensure the sustainability and accessibility of the market. It should also establish a central reporting mechanism for ransomware attacks, to ensure that it has a full understanding of the nature and scale of the threat, and how best to tackle it.

The Home Office claims the lead on ransomware as a national security risk and policy issue, but the former Home Secretary showed no interest in the topic. It has been suggested by some observers that clear political priority in the Home Office is given instead to other issues, such as illegal migration and small boats. In line with many other aspects of cyber security, and to ensure that it is treated as a cross-government national security priority, responsibility for tackling ransomware should be transferred from the Home Office to the Cabinet Office, in partnership with the NCSC and NCA. It should also be overseen directly by the Deputy Prime Minister.

The Government has published an ambitious National Cyber Strategy (NCS), but its progress reporting is currently poor. The National Audit Office (NAO) should review the Government's implementation of the NCS, and the Government should establish a National Security Council sub-committee, to oversee progress against each of the Strategy's five 'pillars' at least twice per year. The Government must also bring forward legislation urgently to update the Computer Misuse Act, which is now over 30 years old.

The National Crime Agency is locked in an uphill struggle against the ransomware threat, with insufficient resources and capabilities to match the scale of this challenge. The Government should invest significantly more resources in the NCA's response to ransomware, enabling it to pursue a more aggressive approach to infiltrating and disrupting ransomware operators. It should also address the pay parity between police and NCA officers, and invest sufficiently in the skills needed to track and seize ransomware criminals' cryptocurrency earnings.

There is a high risk that the Government will face a catastrophic ransomware attack at any moment, and that its planning will be found lacking. If the UK is to avoid being held hostage to fortune, it is vital that ransomware becomes a more pressing political priority, and that more resources are devoted to tackling this pernicious threat to the UK's national security.

1 Introduction

1. On Saturday 8 February 2020, the Leader of Redcar and Cleveland Borough Council received an ominous phone call. A member of Councillor Mary Lanigan's IT team had accessed the Council's system and thought that something didn't "look right". Their instincts were right: the Council had suffered a "catastrophic" ransomware attack and had lost "everything".[1] Social workers were unable to access its systems for managing children's services, including reports about children from concerned members of the public. Councillor (Cllr) Lanigan told us that the Council had "no telephone, no emails, no functioning computers, no laptops, the printers would not work and, crucially, there were no records or documents". The Council refused to pay the ransom, in part to protect other local authorities from similar attacks. Cllr Lanigan told us that its recovery took eight and a half months:

> You can imagine the devastation. I had staff running about with pieces of paper. We brought in another telephone system that we could use, but that took time. It was catastrophic, for the Council and for the residents we serve across the board.[2]

2. Cllr Lanigan's experiences will be familiar to many organisations and institutions across the UK. Our inquiry has found that ransomware—identified by the Government as the UK's foremost cyber security risk[3]—has wrought devastating damage on countless victims and poses a major threat to the UK's national security. This report examines the scale and nature of the threat, how the Government is responding to this challenge, and what more could be done to protect the country from ransomware, support victims to protect themselves and recover from attacks, and tackle the offenders who are profiting so handsomely.

What is ransomware?

3. Ransomware is a type of malicious software—'malware'—designed to damage and destroy computers and computer systems, usually to facilitate extortion. In its most prevalent earlier form, ransomware prevented its victim from accessing their device and/or the data stored on it, by 'encrypting' (effectively locking away) key files or systems.[4] A criminal group would then demand a ransom in exchange for 'decryption', which makes the files available again.[5] Alternatively or in addition to encryption, data might be exfiltrated (effectively taken away or copied), with the ransom demand linked to threats to publish online or sell sensitive data, as outlined in Chapter 2; this form of attack may now be more prevalent, according to some witnesses.[6] The term 'ransomware' has been applied to all stages of the attack, and often encompasses the additional extortion tactics linked to the stolen data.[7]

[1] Q15
[2] Q17
[3] Joint Cybersecurity Advisory (NCSC and others), 2021 Trends Show Increased Globalized Threat of Ransomware, 9 February 2022
[4] Orange Cyberdefense (RAN0029)
[5] National Cyber Security Centre website, Ransomware, accessed 14 August 2023
[6] For example: techUK (RAN0023)
[7] Orange Cyberdefense (RAN0029)

4. The impact of an attack is significant and is experienced both by the primary victim—usually an organisation, which may experience major disruption, reputational damage and financial costs[8]—and by secondary victims, such as members of the public who are blocked from accessing vital services, or customers who find their sensitive data shared online. Ollie Whitehouse, now Chief Technology Officer at the NCSC,[9] told us that "there has never been such a threat that has touched all facets of society, from the very small to the very large".[10] Although there are some instances of individual victims being targeted for smaller sums of money, particularly in earlier iterations of the threat, ransomware is typically experienced by businesses, charities and public sector organisations.[11] We consider the main targets of ransomware in Chapter 2.

Box 1: The main stages of a ransomware attack

David Wall, Professor of Criminology at the University of Leeds, has described the main stages of a ransomware attack:

- Reconnaissance: attackers identify potential victims and the access points within their networks.
- Initial access: this could be obtained via log-in credentials bought on the dark web, or obtained through deception.
- Escalation: once inside, the attackers seek to escalate their access privileges to obtain key organisational data, such as medical or law enforcement records. This might then be extracted and saved by the attackers.
- Activation: the ransomware is installed and activated, locking away key data or systems; at this point, the victim may become aware of the attack. The victim may be 'named and shamed' via the dark web, and they may see a message—like the one displayed in Figure 1—on their device.
- Ransom: the attacker will demand payment, usually in a cryptocurrency such as bitcoin, which is difficult to trace and may subsequently be laundered into more usable currencies. Even if the ransom is paid, the victim may not regain access to all their files.

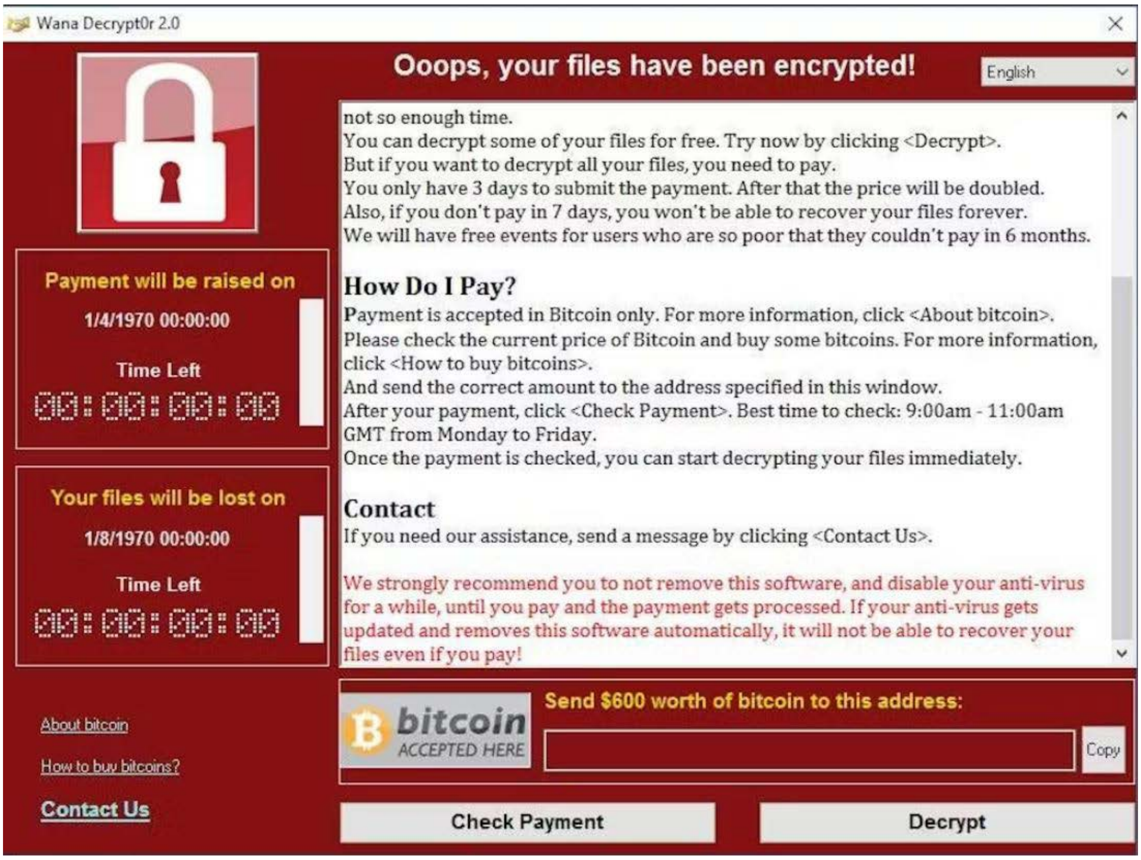
[8] FTI Consulting LLP, Clifford Chance LLP (RAN0034)

[9] And then a representative of NCC Group, a cyber security company

[10] Q1

[11] James Sullivan and James Muir, RUSI Emerging Insights: Ransomware: A Perfect Storm, 29 March 2021

Figure 1: a typical ransom demand



Ooops, your files have been encrypted!

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

Send $600 worth of bitcoin to this address:

Source: David S Wall (The Conversation), Inside a ransomware attack: how dark webs of cybercriminals collaborate to pull them off, 18 June 2021

This Committee and our inquiry

5. The Joint Committee on the National Security Strategy (JCNSS) was established in 2010, with a primary function to "consider the National Security Strategy". Since then, we have fulfilled this task by scrutinising:

- Cross-government national security strategies, the process by which they were created, and the resources allocated to their delivery;
- Discrete policy areas within those strategies; and
- The structures for Government decision-making on national security—particularly the role of the National Security Council (NSC), the National Security Adviser (NSA) and the National Security Secretariat in the Cabinet Office.

6. In the current Parliament, we have undertaken a series of inquiries into how the Government manages specific serious threats to national security, deals with risk management more broadly, and seeks to deliver an effective cross-government response to national security challenges. For example:

- Our December 2020 report on *Biosecurity and national security* examined how the Government had prepared for a pandemic, using Covid-19 as a test case to assess the strength of the UK's national security systems. We found "profound shortcomings" in those systems, including long-present gaps in planning and preparations for biological risks.[12]

- We then looked more broadly at the NSC's ability to make and implement strategy and to plan for crises with rigour. Our September 2021 report on *The UK's national security machinery* found "a troubling lack of clarity" about the NSC's role and remit, as well as "its relationship with other ministerial committees, how it allocates funding for its national security goals, and how it manages the division of responsibilities with the three Devolved Administrations". We also concluded that the rapid fall of Afghanistan to the Taliban in August 2021 indicated that "the NSC and the cross-government machinery that supports its work are inadequate to the task".[13]

- We returned to a narrower focus in 2021/22, examining how the climate risks to our critical national infrastructure (CNI)[14] were being managed. Our subsequent report, *Readiness for storms ahead? Critical national infrastructure in an age of climate change*, found "an extreme weakness at the centre of Government" on this "critical risk to the UK's national security", with no clear ministerial responsibility and a "lax approach" to acting on the Climate Change Committee's findings such that the Government was moving backwards on climate adaptation.[15]

7. Our inquiry into ransomware has enabled us to re-examine a number of those issues through a new lens, including the resilience of UK CNI and the delivery of cross-government strategies. We launched our inquiry in October 2022, informed by a private roundtable of experts. We received 37 pieces of written evidence and held five oral evidence sessions, hearing from experts in cyber security, former victims of ransomware, National Crime Agency (NCA) representatives and Government Ministers. As ever, we benefited

[12] JCNSS, Biosecurity and national security: First Report of Session 2019–21 (HC611/HCL195), 18 December 2020

[13] JCNSS, The UK's national security machinery: First Report of Session 2021–22 (HC231/HL68), 19 September 2021

[14] UK critical national infrastructure (CNI) is defined by the Government's National Protective Security Authority as "those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends". There are 13 CNI sectors in the UK: chemicals, civil nuclear, communications, defence, emergency services, energy, finance, food, government, health, space, transport and water.

[15] JCNSS, Readiness for storms ahead? Critical national infrastructure in an age of climate change: First Report of Session 2022–23 (HC132/HL74), 27 October 2022

enormously from the expertise of our four Specialist Advisers: Paddy McGuinness, Professor Malcolm Chalmers, Professor Michael Clarke and Professor Sir Hew Strachan.[16] We are grateful to all those who contributed to our inquiry.

8. This report is structured around five main chapters. Chapter 2 considers the scale and nature of the ransomware threat, including key trends, targets and perpetrators; we also consider the role of state actors, including the Russian Government. In Chapter 3, we examine the UK's resilience against ransomware, with a particular focus on CNI and local authorities. We then turn to the UK victim experience in Chapter 4, including victim support, insurance, reporting and ransom payments, before scrutinising the Government's strategic response to the ransomware threat in Chapter 5, and to broader cyber security challenges. Finally, in Chapter 6, we consider how to impose costs on ransomware attackers, including through the ability of UK law enforcement to disrupt their operations and to trace and seize the payments they receive from victims.

[16] The four Specialist Advisers declared the following interests. Professor Malcolm Chalmers: Deputy Director-General, Royal United Services Institute. Professor Michael Clarke: Fellow of King's College London (Department of War Studies); Associate Director, Strategy and Security Institute, University of Exeter; Member of the Advisory Boards for: Global Security Forum; Tellus Matrix; Trustee of FAROS charity; Distinguished Fellow, Royal United Services Institute; Fellow, Royal College of Defence Studies; Paid associate of SC Strategy Ltd, Gray's Inn; Partner of Riskology Global, a commercial consultancy on the management of geopolitical and other risks; Contract with Sky News for analysis of war in Ukraine; Fellow of University of Aberystwyth. Paddy McGuinness; Company Director and Founder of Hudhud Associates Limited (Consultancy); Co-Founder of Oxford Digital Health (Healthcare Software provider); Chair of Trustees, St Joseph's Hospice Hackney; Member of the Oxford Board of the Oxford and Cambridge Catholic Education Board; Senior Advisor, Brunswick Group LLC ; Operating Partner, C5 Capital; Advisory Board, Glasswall Solutions; Advisory Board, KAZUAR Advanced Technologies Ltd; Advisory Board, Pool Reinsurance; Senior Adviser, PoolRe/ReNew; Shareholder 2020Partners; US Advisory; Advisory Board member for BlackOut Technologies; Advisor to Strider Intel; Advisory Board, Venari Security; Member Advisory Council of the Azure Forum, Dublin. Professor Sir Hew Strachan; Wardlaw Professor of International Relations at the University of St Andrews; Comité scientifique, Laboratoire de Recherche sur la Défense, IFRI, Paris; Consultant for the Global Strategic Partnership (a consortium led by RAND Europe), commissioned by the Development, Concepts and Doctrine Centre, Ministry of Defence; Patron, British Pugwash Group; HM Lord Lieutenant, Tweeddale; Ambassador for the HALO Trust; Visiting Professor, Royal Norwegian Air Force Academy; Emeritus Fellow, All Souls College, Oxford; Life Fellow, Corpus Christi College, Cambridge; President: Army Records Society, National Army Museum Institute; Co-Chair, Advisory Board, Scottish Council on Global Affairs.

2 The scale and nature of the ransomware threat

9. In November 2014, executives at Sony Pictures received a strange email demanding "monetary compensation", threatening to "bombard" the company if it did not pay. It added: "You know us very well. We never wait long. You'd better behave wisely". Within a few days, Sony employees found themselves unable to access the company's Hollywood studios using their security badges; when they logged into their computers, they were met with an image of a skeleton with the message "Hacked by #GOP". The hackers went on to leak 5,000 emails from the company's Co-Chair Amy Pascal, including unfortunate jokes about Angelina Jolie and Barack Obama.[17]

10. The perpetrators of the Sony hack were later revealed as the North Korean regime's state-funded team of cyber-criminals, the Lazarus Group.[18] This was the first time that their operations had come to the widespread attention of the US public. They were later to become notorious worldwide as the source of the WannaCry ransomware attack in 2017, which affected over 200,000 computers in more than 150 countries.[19] Victims included the UK's NHS, US FedEx, Deutsche Bahn, Honda, Nissan and LATAM Airlines;[20] many, including the NHS,[21] were not targeted specifically by the attackers but were hit due to software vulnerabilities. Despite the number of attacks the Lazarus Group has carried out the group remains persistent, and their capabilities have not been eroded.

11. WannaCry had a huge impact on the NHS, affecting at least 34% of trusts in England.[22] It was estimated to have cost the health service around £92 million through lost services.[23] Thousands of appointments and operations were cancelled, and patients in five areas had to travel to A&E departments elsewhere.[24] Despite its impact, Geoff White, BBC journalist and author of *The Lazarus Heist*, found that WannaCry was only "a dry run for cutting-edge money laundering" for the North Korean hackers: it had made the group very little money, but they had managed to make the cash "disappear" through dozens of online 'crypto wallets', enabling them to launch more profitable attacks in the future.[25]

12. To access its victims' systems and infect them, WannaCry relied on computers using an old version of Windows 7, ruling out organisations with better defences, such as more modern software with appropriate security 'patching'. Five years on, the ransomware threat has evolved rapidly, becoming much more sophisticated and requiring far more advanced defences. The National Cyber Security Centre (NCSC) has now identified ransomware

[17] Geoff White, *The Lazarus Heist,* Penguin: London, 2022

[18] The attack - and the operatives' demands - were linked directly to Sony Pictures production of the 2014 film *The Interview,* in which two journalists are recruited by the CIA to assassinate Kim Jong Un. Source: Geoff White, *The Lazarus Heist,* Penguin: London, 2022

[19] Cloudflare, What was the WannaCry ransomware attack?, accessed 12 September 2023

[20] Acronis, The NHS cyber attack, 7 February 2020; Cloudflare, What was the WannaCry ransomware attack?, accessed 12 September 2023

[21] Department of Health, NHS Improvement and NHS England, Lessons learned review of the WannaCry Ransomware Cyber Attack, February 2018

[22] National Audit Office, Investigation: WannaCry cyber attack and the NHS, 27 October 2017

[23] National Health Executive, WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled, 12 October 2018

[24] National Audit Office, Investigation: WannaCry cyber attack and the NHS, 27 October 2017

[25] Geoff White, The Lazarus Heist, Penguin: London, 2022

as the number one cyber security threat to the UK.[26] This chapter outlines the scale and nature of that threat, including key trends, targets and perpetrators, and the likely role of state actors such as Russia and North Korea.

Key ransomware trends

13. 2021 was described as a "watershed moment" for ransomware,[27] with attackers achieving their "best year ever".[28] One cyber security firm assessed that the number of attacks against UK victims had increased by 233% between 2020 and 2021;[29] the volume of ransom payments also quadrupled.[30] Some of the written evidence for this inquiry suggested that there had been a tailing off of the threat during 2022,[31] but others have asserted that attacks against the UK surged again during 2023, bucking global trends.[32] March 2023 has been assessed as the "worst month on record" for victims whose data has been stolen and posted to "leak sites",[33] with a return to "very high" numbers of incidents.[34]

14. In the face of these conflicting findings, along with low levels of reporting and a lack of official data, we asked the National Crime Agency (NCA) to provide their assessment of the latest ransomware trends. In October 2023, the agency advised us that it saw a "slight decrease" in ransomware attacks after Russia's invasion of Ukraine, followed by a "steady increase". It is "likely" that the number of incidents impacting UK victims has continued to increase during 2023, "reaching the levels seen in 2021". It attributed this in part to two "large scale" attacks this year, against the GoAnywhere file-sharing solution and the MoveIt file transfer solution. The MOVEit exploit alone initially impacted up to 130 organisations and "involved the extraction of the personal information of around sixteen million individuals globally". In a letter to the committee dated 30 November 2023, the NCSC said there were several reasons why there may be more incidents "including better detection, reporting and tracking [of] incidents", but that "this does not necessarily mean the NCSC assess there to be an increased threat from ransomware in the round."[35] This is despite the threat to the UK's critical infrastructure being described as "enduring and significant"[36] by the UK's cyber chief, who was quoted in the NCSC's Annual Review.[37]

[26] Joint Cybersecurity Advisory (NCSC and others), 2021 Trends Show Increased Globalized Threat of Ransomware, 9 February 2022

[27] Spiceworks, Biggest Ransomware Attacks of 2021: A Look Back at the Chart Toppers, 27 January 2022

[28] Q42 (John P. Carlin)

[29] *TechTarget*, SonicWall: Ransomware attacks increased 105% in 2021, 17 February 2022

[30] Financial Action Task Force (FATF), Countering Ransomware Financing, Executive summary, 14 March 2023

[31] For example: FTI Consulting LLP, Clifford Chance LLP (RAN0034)

[32] SonicWall Cyber Threat Report 2023 and Orange Cyberdefense (RAN0029)

[33] A leak site is usually a website on the dark web, requiring a certain browser or software to access content. Dark web leak sites are websites used by ransomware groups, hackers and other malicious actors to leak stolen data and conduct ransom negotiations with victims. Source: Palo Alto Networks, What is a Dark Web Leak Site? Accessed 18 October 2023

[34] Q42 (Jamie MacColl)

[35] National Crime Agency (RAN0041)

[36] National Cyber Security Centre, NCSC warns of enduring and significant threat to UK's critical infrastructure, 14 November 2023

[37] UK Government (RAN0042)

15. Witnesses were almost unified on the changing nature of the threat, describing the evolution of a mature and complex ecosystem[38] with a "cell-like architecture,[39] akin to other forms of serious organised crime.[40] Key developments include:

- The growth in **ransomware-as-a-service** (RaaS), in which an efficient division of labour has evolved.[41] Typically, 'initial access brokers' will achieve the initial hack and sell the access onto 'affiliates'; ransomware operators will also sell a malware source code to affiliates (and might also negotiate with victims); and affiliates will then pay a service fee to ransomware operators for every collected ransom.[42] These 'groups' of actors are connected in quite loose ways,[43] making attribution of responsibility for attacks more difficult.[44] This efficiency of specialisation has increased the tempo of ransomware operations.[45] It has also lowered the cost barrier to entry into ransomware,[46] because less sophisticated criminal groups (affiliates) can purchase the required technology to conduct more advanced attacks.[47] One witness described the typical threat actor now as "quicker, more agile and brazen".[48]

- **Innovations in marketing, recruitment and communication**:[49] RaaS operatives are known to offer their services on a monthly subscription basis with optional extras, and have actively recruited affiliates.[50] Groups operate on closed chatrooms to communicate with one another,[51] and some even act like legitimate enterprises, establishing HR functions to coordinate their annual leave.[52]

- A shift towards larger, higher-value targets (sometimes described as "**big game hunting**"),[53] with threat actors developing more "sophisticated weaponry" and achieving much larger ransom pay-outs.[54]

- An increase in **double or triple extortion** methods (touched upon in Chapter 1), in which ransom demands are linked to threats to publish sensitive data online;[55] in these cases, the data may be "exfiltrated" (removed) rather than encrypted.[56] Organisations are thus held to ransom on the grounds of confidentiality (release of sensitive data), and not just availability (access to files).[57] In triple extortion, the victim's customers or suppliers may be threatened with the release of sensitive

[38] Q2 and NCC Group (RAN0012)
[39] Q3
[40] Q5 (Professor Sadie Creese)
[41] BAE Systems (RAN0014), NCC Group (RAN0012), FTI Consulting LLP, Clifford Chance LLP (RAN0034), Palo Alto Networks (RAN0033)
[42] NCC Group (RAN0012)
[43] Q3
[44] Q2
[45] James Sullivan and James Muir, RUSI Emerging Insights: Ransomware: A Perfect Storm, 29 March 2021
[46] Q53 (Graeme Biggar)
[47] CrowdStrike (RAN0017)
[48] CrowdStrike (RAN0017)
[49] James Sullivan and James Muir, RUSI Emerging Insights: Ransomware: A Perfect Storm, 29 March 2021
[50] FTI Consulting LLP, Clifford Chance LLP (RAN0034)
[51] Q3
[52] NCC Group (RAN0012)
[53] FTI Consulting LLP, Clifford Chance LLP (RAN0034)
[54] Q7
[55] Q7, NCC Group (RAN0012), CrowdStrike (RAN0017)
[56] Q53 (Graeme Biggar)
[57] James Sullivan and James Muir, RUSI Emerging Insights: Ransomware: A Perfect Storm, 29 March 2021

data if they do not pay a further ransom;[58] a "premium subscription" might also be on sale—to the victim and others—in exchange for exclusive rights over the data.[59]

16. There was some speculation among witnesses about how the ransomware threat might evolve in future. Future trends could include:

- A move towards targeting larger operators of CNI (operational technology and IT),[60] alongside threats of sabotage to operations—this would be particularly risky in relation to CNI, where such attacks could cause "a threat to physical security or safety of human life";[61]
- The possibility that ransomware operators might access 'cyber-physical systems', such as the control, steering and throttle on a shipping vessel (lab experiments have demonstrated that this is achievable);[62]
- A move towards data corruption, in which data is manipulated to be misleading or to contribute to disinformation campaigns (undermining its integrity) before being posted online[63]—this could also utilise the increasingly sophisticated 'deepfake' videos or audio being produced through generative AI techniques;[64]
- The possible targeting of smart devices (the so-called 'Internet of Things'), with attacks spreading to other devices within a network;[65] and
- A focus on cloud service providers, on which UK CNI businesses are increasingly reliant.[66]

Key targets

17. The UK is one of the most targeted countries in the world for ransomware, with some estimates putting it second only to the US.[67] None of our witnesses were able to shed much light on why the UK is victimised more than other major European economies. When we asked Ministers and the NCSC, the Minister for Security said:

> There is a very simple reason: the English Language. Then there is a more prosaic reason which is our open banking systems. The combination of the two means that the UK is particularly targeted by those who are able to communicate with us and who can see that they can quickly move any ransoms taken into different banking systems and outside the jurisdiction of the United Kingdom.[68]

[58] *Security Intelligence*, Triple extortion and erased data are the new ransomware norm, 20 April 2023

[59] STORM Guidance Limited (RAN0001)

[60] Dr Matthew Shillito (Lecturer in Law at University of Liverpool) (RAN0025)

[61] Q7 (Prof Sadie Creese)

[62] Cyber-SHIP Lab, University of Plymouth (RAN0016)

[63] FTI Consulting LLP, Clifford Chance LLP (RAN0034)

[64] *Wired*, Brace Yourself for the 2024 Deepfake Election, 27 April 2023

[65] PlatinumHIT (RAN0026)

[66] FTI Consulting LLP, Clifford Chance LLP (RAN0034)

[67] NCC Group (RAN0012)

[68] Q67

18. On the 4 December the Government confirmed their commitment to provide "up to £10 million of new funding for research on risks to the economy and our public finances".[69] However, until this funding has been delivered and utilised, the current evidence paints a mixed picture of which organisations are most likely to experience ransomware attacks and is limited by a lack of reporting. Last year, the education sector was identified as one of the top UK targets within a joint trends report by the FBI, NCSC and their Australian counterparts, but the NCSC also reported attacks against businesses, charities, the legal profession, local government and health organisations.[70] Some submissions to our inquiry claimed that industrial and manufacturing organisations were the most attacked targets,[71] with others identifying education, retail and law.[72] A more recent analysis of global trends found that the media, entertainment and leisure sectors had become the most victimised organisations worldwide, followed by retail and energy infrastructure.[73]

19. Although the UK has so far avoided a 'C1 attack'[74]—the highest categorisation of attack severity used by the Government—a number of international examples have demonstrated the severe damage that can be wrought on public services by ransomware. For example:

- In May 2021, the **Health Service Executive (HSE) of Ireland** became aware of a major cyber-attack against its IT systems.[75] Attackers encrypted 80% of HSE's IT,[76] using ransomware linked to the Russian-speaking ransomware group Conti.[77] Staff had no access to diagnostics or medical records, and had to revert to pen and paper. It took four months for the organisation to recover fully from the attack,[78] and press reports suggest that it has cost taxpayers at least €101 million (approximately £87 million).[79] John Ward, Interim Chief Technology and Transformation Officer for HSE, told us that the incident had generated risks to patient care, with doctors unable to access scans and clinical notes.[80]

- As outlined in Chapter 5, the **US Government** declared a state of emergency in May 2021 when one of its major oil pipelines, **Colonial Pipeline**, was shut down for six days after a ransomware attack, affecting 17 US states and causing fuel shortages, panic buying and flight re-routings.

- Last year, **Costa Rica** was also forced to declare a state of emergency after a month of catastrophic ransomware attacks, affecting its systems for tax collection, customs and social security.[81]

[69] HMG, The UK Government Resilience Framework Implementation update, 2023, p21 HMG

[70] Joint Cybersecurity Advisory (NCSC and others), 2021 Trends Show Increased Globalized Threat of Ransomware, 9 February 2022

[71] BAE Systems (RAN0014), NCC Group (RAN0012)

[72] JUMPSEC, UK Ransomware Trends 2022, accessed 22 September 2023; Orange Cyberdefense (RAN0029)

[73] *Tech Target*, Top 13 ransomware targets in 2023 and beyond, accessed 22 September 2023

[74] Q66 (Graeme Biggar)

[75] HSE Ireland, Conti cyberattack on the HSE, 3 December 2021

[76] HHS Cybersecurity Program, Lessons Learned from the HSE Cyber Attack, 2 March 2022

[77] HSE Ireland, Conti cyberattack on the HSE, 3 December 2021

[78] HHS Cybersecurity Program, Lessons Learned from the HSE Cyber Attack, 2 March 2022

[79] *Irish Independent*, HSE cyber attack cost taxpayers at least €101m, with a further €657m to be spent safeguarding against repeat attacks, 30 September 2022

[80] Q17

[81] *The Guardian*, Costa Rica declares national emergency amid ransomware attacks, 12 May 2022

20. In light of these devastating attacks, we were keen to establish the extent of UK CNI's vulnerability to a ransomware attack, and whether it was likely to be targeted by threat actors. As outlined in Chapter 3, we uncovered major concerns about the resilience of UK CNI to ransomware, which Graeme Biggar described as "the one serious organised crime that could bring the country to a standstill".[82] Modelling by the Office for Budget Responsibility (OBR) has also found that a major UK cyber-attack (which might take the form of a ransomware attack) could result in a shock to the economy of 1.6% of GDP, adding £29 billion to Government borrowing.[83] It based its findings on a scenario in which a cyber-attack causes severe disruption to the electricity grid in the South East of the UK, including London, causing 'rolling blackouts' for three weeks. The OBR predicted that direct Government support provided during the crisis period would amount to approximately £16 billion, with the economy taking a year to recover.[84]

21. **A major ransomware attack could have a devastating impact on UK citizens and the economy, and undoubtedly represents a major threat to UK national security. A sophisticated ransomware ecosystem has evolved, with criminals able to purchase advanced forms of malware and access points in order to conduct profitable and damaging attacks. This has made it much more widely available to those who wish to inflict harm for profit, and increased the scale of the threat.**

22. **Past attacks demonstrate that ransomware can cause severe disruption to the delivery of core Government services, including healthcare and child protection, as well as causing ongoing economic losses. Mass data loss from an attack can be irreversible, even when the ransom is paid. Given the damage wrought by these uncoordinated ransomware attacks, a coordinated and targeted attack has the potential to take down large parts of the UK's critical national infrastructure and public services and—in the words of the National Crime Agency—to bring the country to a standstill. It would also shine a spotlight on the inadequacy of the Government's efforts to secure the UK against ransomware, and to prepare for the aftermath of a major cyber-attack.**

Who is conducting most ransomware attacks?

23. In February 2015, the FBI issued a 'most wanted' notice for the Russian cyber-criminal Evgeniy Mikhailovich Bogachev, offering US$3 million for information leading to his arrest or conviction. The 39-year-old Russian national was last known to live in Anapa, a town on the northern coast of the Black Sea, and is believed to enjoy boating. Eight years on, he remains wanted for his involvement in the GameOver Zeus ransomware strain, thought to be responsible for over a million computer infections and for financial losses of more than US$100 million.[85]

24. It is unclear how representative Mr Bogachev is of the average ransomware operator. Witnesses emphasised the disparate and amorphous nature of the ransomware ecosystem: there is "not one global head of ransomware by any stretch", but rather "loose affiliations of people", and "those affiliations change over time".[86] What is much clearer, however, is the dominant role of Russian-speaking actors. For example:

[82] Q54

[83] OBR, Fiscal risks and sustainability, July 2022 (p7)

[84] OBR, Fiscal risks and sustainability, July 2022 (p54–56)

[85] FBI website, Most Wanted: EVGENIY MIKHAILOVICH BOGACHEV, accessed 22 September 2023

[86] Q3

- The NCSC's 2022 Annual Review noted that most of the ransomware groups targeting the UK are "based in and around Russia", benefiting from "the tacit consent of the Russian State";[87]
- The NCSC's Annual Review 2023 raised the same concerns but placed emphasis on the development of "a new place of cyber adversary" who are often "sympathetic to Russia's further invasion of Ukraine and are ideologically, rather than financially motivated".[88]
- In its written evidence to this inquiry, the Government stated with near certainty that "the deployment of the highest impact malware (including ransomware) affecting the UK remains concentrated mostly in Russia";[89] and
- DXC Technology, a US IT company, told us that, of the ten most prolific and dangerous ransomware strains identified by the NCSC's Ransomware Threat Assessment Model, eight are "likely based in Russia".[90]

According to RUSI, some of these groups are experienced in this evolving field of offending: in many cases, the same Russian actors were conducting "malware and botnet operations" against UK financial institutions from 2010 onwards, and have subsequently "pivoted their business model" towards ransomware operations.[91] The lines between state activity and criminal groups are also blurred, as we examine in further detail below.

25. Prior to Putin's full-scale 2022 invasion of Ukraine, it harboured an element of the ransomware threat: Jamie MacColl from RUSI commented that the ransomware ecosystem contained "multiple nationalities from former Soviet Union countries, including Ukraine".[92] The NCA told us that it had worked with the Ukrainian Government in the past to investigate and arrest some of those offenders, but that the Ukrainian attackers had subsequently either gone to Russia or had "turned to attacking Russia", rather than the West.[93] The impact of the war on cyber threat levels overall appears mixed: a reported wave of cyber-attacks against Ukraine encountered strong defences,[94,95] and some downward global trends have been attributed to the war distracting Russian aggressors away from conducting ransomware attacks.[96] It has also caused splits within ransomware groups, with members coming out for and against the Russian Government. This splintering may have made such groups even harder to disrupt.[97]

The role of state actors globally

26. WannaCry has caused inseparable links, in the minds of many observers, between the ransomware threat and the People's Republic of North Korea. Geoff White's depiction of the Lazarus Heist, outlining the role of the North Korean regime in training young

[87] NCSC, Annual Review 2022, 1 November 2022
[88] NCSC, Annual Review 2023, 14 November 2023
[89] Cabinet Office (RAN0018)
[90] DXC Technology (RAN0035)
[91] Royal United Services Institute (RAN0032)
[92] Q35 (Jamie MacColl)
[93] Q58
[94] Centre for Strategic & International Studies (James Andrew Lewis), Cyber War and Ukraine, 16 June 2022
[95] Q58 (Graeme Biggar)
[96] Q37 (John P. Carlin)
[97] Q37 (Jamie MacColl)

ransomware operatives, painted a vivid picture of the potential for governments to use ransomware as a revenue-raising exercise, training their brightest young mathematicians and computer scientists to become weapons of the state.[98]

27. Witnesses were clear, however, that the ransomware threat from other countries remains relatively small in comparison with Russia.[99] For example:

- **China** is considered the single most significant cyber security actor in relation to UK interests—the NCSC noted last year that it was "becoming ever more sophisticated, increasingly targeting third-party technology, software and service supply chains"[100]—but Graeme Biggar told us that it has "tended to use its capabilities for state espionage and theft of intellectual property rights", rather than ransomware attacks.[101] We received no evidence that China was serving as a host for more independent ransomware attackers, as Russia has done. (In contrast, the White House said in 2021 that hackers working for Chinese intelligence agencies had played a role in ransomware attacks against US businesses.[102])

- As outlined above, **North Korea** has used ransomware with some success through the Lazarus Group and other state-sponsored cyber-criminals,[103] but it is now described by NCSC as "a less sophisticated cyber aggressor".[104]

- **Iran** is an "aggressive cyber actor"[105] and has some impressive capabilities, which it has used "for actions that are on the bridge between state crime and espionage",[106] but its levels of ransomware activity are dwarfed by those of Russian actors.[107] Iranian threat actors have relied on using published vulnerabilities to gain access to 'unpatched' systems, rather than more advanced intrusion tactics.[108]

The role of the Kremlin

28. The dominance of Russian-speaking ransomware actors has inevitably generated questions about the Russian state's role in the proliferation of attacks. The Kremlin's approach to foreign policy was described by the Intelligence and Security Committee (ISC) in 2020 as a "zero-sum game", with any actions damaging to the West seen as "fundamentally good for Russia". This "nihilistic" attitude makes it particularly difficult for the West to manage the security threat posed by the Kremlin.[109] The Government's

[98] Geoff White, The Lazarus Heist, Penguin: London, 2022
[99] For example, Q6
[100] NCSC, Annual Review 2022, November 2022
[101] Q58 (Graeme Biggar)
[102] *NBC News*, U.S. accuses China of abetting ransomware attack, 19 July 2021
[103] Q58 (Graeme Biggar)
[104] NCSC, Annual Review 2022, November 2022
[105] NCSC, Annual Review 2022, November 2022
[106] Q58 (Graeme Biggar)
[107] Q6 (Ollie Whitehouse)
[108] NCSC, Annual Review 2022, November 2022
[109] Intelligence and Security Committee of Parliament, Russia (HC 632), 21 July 2020

2021 Integrated Review (IR) of Security, Defence, Development and Foreign Policy and its 2023 IR 'Refresh' (IRR) both identified Russia as the most acute threat to the UK's security.[110]

29. The Kremlin's relationship with organised criminal groups in Russia is also well established. In a book that prompted extensive litigation, *Putin's People*, Catherine Belton (a former Moscow Correspondent for the *Financial Times*) documented the manner in which Putin and his former KGB colleagues took over Russia's economy and state institutions, and blurred the lines between organised crime and political power.[111] Professor Mark Galeotti, Senior Associate Fellow at RUSI, has also described how "organised crime prospers under Putin, because it can go with the grain of his system"; high levels of corruption provide a "conducive environment", and state agents also exploit criminal opportunities to line their own pockets. The criminal gangs that prosper in today's Russia "tend to do so by working with rather than against the state. In other words: do well by the Kremlin, and the Kremlin will turn a blind eye".[112]

30. Clear links have also been established between Russian cyber-criminals and the Kremlin, and some legal analysts have assessed that Russia's approach to cybercrime *could* constitute a violation of international law and poses and advanced persistent threat .[113] For example:

- In 2021, the US Treasury Department said that the Russian FSB "cultivates and co-opts criminal hackers", enabling them to "engage in disruptive ransomware attacks and phishing campaigns".[114] Please note in chapter 6 our report focuses on the mechanism international law can provide but that at present the UK is without a clear process for prosecuting attackers.

- In an *Associated Press* (AP) analysis published the same year, former CIA analyst Michael van Landingham said: "Like almost any major industry in Russia, [cyber-criminals] work kind of with the tacit consent and sometimes explicit consent of the security services". Sometimes, "the hackers use the same computer systems for state-sanctioned hacking and off-the-clock cybercrime for personal enrichment".[115]

- In March, a consortium of 11 media outlets, including *The Guardian*, revealed the extent of cooperation between Russian authorities and cyber-criminals. Described as the 'Vulkan files', these materials show the connections between Russian intelligence and agencies and the cyber security company Vulkan,

[110] HM Government, Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy (CP 403), March 2021; HM Government, Integrated Review Refresh 2023: Responding to a more contested and volatile world (CP 811), March 2023

[111] Catherine Belton, *Putin's People: How the KGB took back Russia and then took on the West,* Harper Collins: London, 2020

[112] *The Guardian* Long Read (Mark Galeotti), Gangster's paradise: how organised crime took over Russia, 23 March 2018

[113] For example: Harriet Moynihan (Chatham House), The Application of International Law to State Cyberattacks, 2 December 2019; Cyber Law Toolkit website (University of Exeter and others), Scenario 14: Ransomware campaign, accessed 28 September 2023

[114] US Department of the Treasury press release, Treasury Sanctions Russia with Sweeping New Sanctions Authority, 15 April 2021

[115] AP, How the Kremlin provides a safe harbor for ransomware, 16 April 2021

which in turn is linked to the notorious hacking group Sandworm.[116] Vulkan is part of Russia's "military-industrial complex", receiving Government licenses to work on classified military projects.[117]

31. In relation to any single attack or threat actor, however, it may be difficult to unpick links to the Kremlin. This has implications for general understanding about the nature of the threat and the purpose of some attacks, and for the ability to attribute responsibility. John P. Carlin, former acting US Deputy Attorney General, described ransomware as a "blended threat": a criminal actor might conduct an attack to "make a buck", but the same actor might be "leveraged" by the state that was giving it safe harbour (Russia or otherwise) to "commit attacks consistent with the goals of the state".[118] The Government also told us that state involvement in attacks varies, from "knowledge of ransomware OCGs' [organised criminal groups'] criminal activity and allowing them to operate with impunity" to "more direct links", such as "the deep relationship between ransomware group Evil Corp and the Russian Federal Security Service (FSB)."[119] It nevertheless described ransomware actors as "financially motivated" rather than politically directed, echoing a number of other witnesses' assessment of Russian operatives' main motive for attacking Western targets.[120,121] This has also been posited as one reason why ransomware attacks (as opposed to cyber-attacks more broadly) have not been conducted in large numbers against Ukrainian targets, which would be unlikely to pay ransoms to Russian criminal groups.

32. **Russian-speaking actors are the source of most attributable ransomware attacks against UK targets. The Russian Government's tacit (or even explicit) approval of these attacks is consistent with the Kremlin's disruptive, zero-sum-game approach to the West. It also provides revenue to the Putin regime's well-oiled network of corruption and criminality. This is not a straightforward state threat, however. For many Russian hackers, ransomware is simply an easy way to make large sums of money, with next-to-no chance of being caught or prosecuted. Regardless of the extent of state involvement, or whether they are ideologically driven rather than financially, the sheer scale of the threat demonstrates how vital it is that the UK is adequately resourced to upscale its defences, and to prepare for a major attack.**

[116] *The Guardian*, 'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics, 30 March 2023
[117] *The Guardian*, 'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics, 30 March 2023
[118] Q35 (John P. Carlin)
[119] Cabinet Office (RAN0018)
[120] E.g. techUK (RAN0023), Chainalysis Inc. (RAN0008)
[121] Council on Foreign Relations (blog post), Financial Incentives May Explain the Perceived Lack of Ransomware in Russia's Latest Assault on Ukraine, 26 July 2022

3 Strengthening our defences—UK preparedness and resilience

33. In April 2022, the Government of Costa Rica was hit by a widescale ransomware attack that affected 27 government departments over the course of several weeks. The President declared a state of national emergency and said that the country was "at war" with the attackers. It reportedly left parts of Costa Rica's digital infrastructure "crippled for months, paralysing online tax collection, disrupting public healthcare and the pay of some public sector workers".[122] Unsurprisingly, the economic damage was also significant: it was estimated by one congresswoman to have cost the Costa Rican economy approximately US$30 million dollars per day, and the Costa Rican Chamber of Foreign Commerce estimated losses of over US$125 million in the first two days alone.[123]

34. The UK has yet to experience a coordinated attack across multiple elements of its critical national infrastructure, so the Government's response remains largely untested—but the Costa Rican experience shows how rapidly a nation can be brought to its knees by such a widescale assault on its digital infrastructure. This chapter considers the UK's defences against the ransomware threat, and what more could be done to protect UK CNI—and the UK economy more broadly—from major ransomware attacks.

The resilience of UK critical national infrastructure

35. UK CNI is critical to the smooth running of the economy and society. The Government's 2023 National Risk Register (NRR) recognises that cyber-attacks on infrastructure pose a serious risk to national security: it assessed the likelihood of such an attack occurring (over a two-year timeframe) as 5–25%, and the impact as "moderate"—putting it in the same category as a terrorist attack on transport, a medium-scale chemical or nuclear attack, or a major contamination of UK food supply.[124]

36. A number of recent attacks have demonstrated the ongoing vulnerability of UK CNI to ransomware. For example:

- **Royal Mail** found its export services "paralysed for weeks" after a ransomware attack in January 2022, with knock-on effects on small businesses that rely on it to ship products overseas.[125]

- During a period of drought in August 2022, **South Staffordshire Water** was targeted by ransomware actors who claimed to have accessed systems that control industrial processes at the company's water treatment plants.[126]

- The **Advanced** software provider, which supports **NHS 111** and other patient systems, also found itself under attack in August 2022. The attack forced doctors to revert to pen and paper for months, and left patient care "badly affected" in some care settings.[127]

[122] *Financial Times*, How Conti ransomware group crippled Costa Rica — then fell apart, 9 July 2022
[123] *Rest of World*, A massive cyberattack in Costa Rica leaves citizens hurting, 1 June 2022
[124] HM Government, National Risk Register: 2023 edition
[125] *Computer Weekly*, Royal Mail resumes full export service after cyber attack, 21 February 2023
[126] FTI Consulting LLP, Clifford Chance LLP (RAN0034)
[127] *BBC News*, Advanced cyber-attack: NHS doctors' paperwork piles up, 30 August 2022

- In September 2023, it was reported that the Lockbit ransomware group had released data from the **Ministry of Defence** after an attack on a metal fencing company, Zaun, which supplied sites such as the Porton Down research unit.[128]

- Later that month, the personal details of police officers from **Greater Manchester Police** were obtained in a ransomware attack against a company that makes ID cards.[129]

37. The NCSC—a wing of GCHQ—is the UK's national technical authority for cyber security,[130] and aims to "make the UK the safest place to live and work online",[131] working in partnership with the Cabinet Office and the 'Lead Government Departments' for different CNI sectors. This work is delivered through a number of initiatives, including:

- The Government's Cyber Essentials Scheme, which provides two levels of voluntary certification, through which businesses and other organisations can self-assure about their levels of resilience against cyber-attacks;[132]

- The NCSC's Cyber Assessment Framework (CAF), which provides guidance for companies that operate "vitally important services and activities", including UK CNI;[133]

- The NCSC's ransomware portal, which contains "advice and guidance, including practical resources to help users prevent, report, respond to and recover from attacks";[134]

- The NCSC's free Early Warning service, which monitors multiple sources and delivers notifications about possible system compromise, malicious activity and vulnerabilities;[135]

- A recently-established NCSC CNI alert, offering guidance to help CNI organisations to understand emerging cyber threats, and a scheme for assessing the resilience of CNI operators (through conducting attack simulation exercises);[136]

- Expansion of the NCSC's accreditation scheme for Cyber Incident Response companies; and

- A Cyber Awareness campaign to improve the public's understanding of cyber security risks, which received 1.2 million views in two and a half years.[137]

[128] *Computer Weekly*, LockBit ransomware gang allegedly leaks MoD data after hit on supplier, 4 September 2023

[129] *BBC News*, Greater Manchester Police officers' details hacked in cyber attack, 14 September 2023

[130] More fully, the NCSC is the UK's "national technical authority for information assurance which provides advice and assistance on cyber security in accordance with its functions under the Intelligence Services Act 1994". From NCSC website, NCSC CAF guidance, accessed 6 October 2023

[131] NCSC, Annual Review 2022, November 2022

[132] NCSC website, About Cyber Essentials, accessed 28 September 2023

[133] NCSC website, NCSC CAF guidance, accessed 26 September 2023

[134] Cabinet Office (RAN0018)

[135] NCSC Early Warning website, accessed 28 September 2023

[136] Cabinet Office (RAN0018)

[137] Cabinet Office (RAN0018)

The Cabinet Office also hosts the CNI Knowledge Base, which it describes as "the 'Single Source of Truth' for UK CNI", enabling government analysts and risk owners (e.g. in Lead Government Departments) to "view UK CNI on a map or as a network graph, with interdependencies mapped across it".[138]

38. Despite this considerable programme of work, witnesses outlined major concerns about CNI preparedness and resilience. They told us that:

- In the context of "ever-increasing digitalisation of the UK's CNI operations",[139] **many CNI operators are still operating outdated legacy systems**. According to Thales, it is "not uncommon" to find ageing systems within CNI organisations with a long operational life, which are "not routinely updated, monitored or assessed".[140] The increase in hybrid and remote working also brings additional risks.[141]

- **Legacy operational technology** (OT)[142] poses a particular challenge: digital transformation is resulting in these assets, which were "never designed with smart functionality in mind", being "overlayed with IT and hyper connectivity". OT systems are "much more likely to include components that are 20 to 30 years old and/or use older software that is less secure and no longer supported".[143] Thales is seeing "increased [threat actor] activity across all of the critical national infrastructure sectors", with a move towards attacks on certain types of OT.[144] Reliance on digital systems also means that attacks against operators' wider IT systems can force companies to shut down their OT[145]—as in the case of the US Colonial Pipeline attack, in which the affected systems were responsible for corporate functions such as billing and accounting.[146]

- **The NHS remains particularly vulnerable**: healthcare is a "large and growing target across Europe",[147] and the NHS operates a "vast estate of legacy infrastructure", including "IT systems that are out of support or have reached the end of their lifecycle". This puts it in a "particularly difficult position to protect itself from cyber-attacks",[148] despite the fact that many critical medical devices and equipment are now connected to the internet.[149] Many hospitals

[138] Cabinet Office, NCSC and NPSA, Improving our understanding of Critical National Infrastructure (industry flyer), accessed 28 September 2023

[139] FTI Consulting LLP, Clifford Chance LLP (RAN0034)

[140] Thales (RAN0019)

[141] (ISC)2 (RAN0010)

[142] According to CISCO, "Operational technology (OT) is the hardware and software that monitors and controls devices, processes, and infrastructure, and is used in industrial settings. IT combines technologies for networking, information processing, enterprise data centers, and cloud systems. OT devices control the physical world, while IT systems manage data and applications." From: CISCO website, How Do OT and IT Differ? Accessed 18 October 2023

[143] NCC Group (RAN0012)

[144] Thales (RAN0019)

[145] JUMPSEC (RAN0009)

[146] *Tech Target*, Colonial Pipeline hack explained: Everything you need to know, 26 April 2022

[147] CrowdStrike (RAN0017)

[148] PlatinumHIT (RAN0026)

[149] Dr Suresh Renukappa (Senior Lecturer at University of Wolverhampton); Mr Chandrashekar Subbarao (Researcher at University of Wolverhampton); Dr Subashini Suresh (Reader at University of Wolverhampton) (RAN0013)

lack the capacity to undertake even "simple upgrades" as a result of crumbling IT services and a lack of investment.[150] The Advanced attack (outlined above) also demonstrates the additional vulnerabilities created by NHS supply chains.

39. Some of the developments outlined in Chapter 2 have also left CNI more vulnerable to attack. Alongside a growth in more targeted attacks,[151] ransomware-as-a-service (RaaS) can involve a more "chaotic" approach to attacking victims,[152] meaning that CNI operational technology may be hit by accident. Ransomware groups were described by one witness as "vultures not hawks": incidents can be the result of "control gaps", and attacks may be opportunistic rather than targeted, with attackers not always knowing which network they have accessed.[153] The NCSC also stressed recently that most cyber-criminals do not target specific sectors or organisations, but rather "take the opportunities presented to them".[154]

40. Despite this, the UK and its CNI are facing an ever-more sophisticated threat actor. The main ransomware strains targeting the UK between 2020 and 2022, Conti and Lockbit, are "some of the world's most sophisticated", responsible for "attacks at the cutting edge of the field".[155] As a result, we were told that ransomware operators are now "considerably out-pacing victim organisations' under-funded, overworked security and IT teams".[156] Even the "most diligent" organisation might have "hundreds of thousands of devices"; "complete 100% patching of those devices is simply not achievable", meaning that some attacks will succeed.[157]

41. Speaking to us in June, senior NCA officials voiced particular concerns about the vulnerability of CNI operators' supply chains, noting that there is a soft 'underbelly' to every organisation that uses a third-party software provider. Rob Jones, Director General of Operations at the NCA, described this as "the unsurfaced risk in an element of the supply chain", which could undermine the investment in defence and resilience. It is "what worries us most", and could cause a "quite significant" incident. Major concerns about CNI supply chains were also expressed by a number of witnesses,[158] with some noting that small and medium sized enterprises (SMEs) often have particularly poor defences against cyber-attacks.[159]

42. The net result of these vulnerabilities is that, if too many CNI operators were to fall victim at once, the UK might struggle to respond: according to Professor Sadie Creese from the University of Oxford, as a result of the "underinvestment" outlined above, UK authorities would "find it very hard to deploy the levels of support necessary to avoid very large amounts of harm" in those circumstances.[160] PwC also noted the potential for more

[150] PlatinumHIT (RAN0026)
[151] Cabinet Office (RAN0018)
[152] Q53 (Rob Jones)
[153] Secureworks (RAN0036)
[154] NCSC and NCA, Ransomware, extortion and the cyber crime ecosystem: A white paper from the NCSC and the NCA, 11 September 2023
[155] FTI Consulting LLP, Clifford Chance LLP (RAN0034)
[156] CrowdStrike (RAN0017)
[157] Mr Andrew Jones (RAN0002)
[158] For example: NCC Group (RAN0012), DXC Technology (RAN0035), Q7 (Jayan Perera)
[159] For example: Q7 (Jayan Perera), CrowdStrike (RAN0017)
[160] Q9 (Professor Sadie Creese)

severe damage to be wrought by a "directed campaign targeted at UK interests" (which might then cover several sectors at once), rather than the threat from more disparate criminal groups.[161]

43. **The Government and the National Cyber Security Centre (NCSC)—the public-facing arm of GCHQ—have focused significant efforts on enhancing the UK's cyber resilience, with particular attention paid to major operators of critical national infrastructure (CNI). Nevertheless, UK CNI remains vulnerable to a catastrophic ransomware attack, particularly in sectors in which investment in upgrading legacy infrastructure has been inadequate. Supply chains are also particularly vulnerable, and have been described by the NCA as the 'soft underbelly' of CNI. With different CNI operators sharing the same supplier, a single attack could also affect multiple sectors at once, with damaging and widespread consequences.**

Regulatory requirements

44. JCNSS has long taken a strong interest in the regulatory requirements placed on CNI operators, which are a key lever for achieving higher resilience standards. Our 2022 report on CNI and climate adaptation argued that the Government had been far too reluctant to impose stricter resilience requirements on CNI operators, expressing particular concerns about the significant interdependencies between sectors.[162] We endorsed the findings of the National Infrastructure Commission, which called for the Government to publish a full set of resilience standards every five years, following advice from regulators. We also raised serious concerns[163] when the Resilience Framework, published in December 2022, appeared to delay imposing any new resilience regulations on CNI operators until after 2030, committing instead to "review existing regulatory regimes" by that date.[164]

45. Cyber resilience is one area in which there is already some legislative harmony across multiple CNI sectors, however, thanks to the Network & Information System (NIS) regulations. These legal measures, which were the result of an EU directive and were initially introduced in 2018,[165] aim to boost the overall level of security (both cyber and physical resilience) of network and information systems that are "critical for the provision of essential services and digital services",[166] by requiring operators to take appropriate and proportionate security measures to manage risks to their networks and information systems.[167] The NIS regulations cover large parts of UK CNI, including healthcare, transport, energy and water,[168] and similar requirements are also in place for the finance, telecommunications, civil nuclear and chemicals sectors.[169]

46. Despite the wide scope of the NIS regulations, a large number of submissions called for the Government to strengthen its regulatory oversight of cyber resilience.[170] For example,

[161] PwC UK (RAN0006)

[162] JCNSS, Readiness for storms ahead? Critical national infrastructure in an age of climate change: First Report of Session 2022–23 (HC132/HL74), 27 October 2022

[163] JCNSS news article, Climate change impacts on infrastructure – Committee calls for greater government urgency, 2 March 2023

[164] HM Government, The UK Government Resilience Framework, December 2022

[165] NCSC website, NCSC CAF guidance: NIS introduction, accessed 28 September 2023

[166] Gov.uk, The NIS Regulations 2018, last updated 4 January 2023

[167] NCSC website, NCSC CAF guidance: NIS introduction, accessed 28 September 2023

[168] Schedule 2 of the Network and Information Systems Regulations 2018

[169] Correspondence from the Deputy Prime Minister to the Chair of JCNSS, 10 July 2023

[170] Including: Association of British Insurers (RAN0021), NCC Group (RAN0012), Thales (RAN0019)

NCC Group argued for the use of "proportionate regulatory levers" to roll out "basic cyber hygiene", arguing that regulation in the financial sector has reduced the number of ransomware incidents,[171] and Thales called for "increased regulatory influence over CNI owners and operators".[172] The Government's own Cyber Breaches survey also found recently that only half of surveyed medium-sized businesses and 59% of large businesses had even heard of the NCSC's Cyber Essentials standard in 2022, let alone implemented it.[173]

47. The Government's 2022 National Cyber Strategy acknowledges that it needs to "set clear expectations" on cyber resilience for CNI businesses, "underpinned by the right framework of incentives, support and regulation to enable improvement". It makes the following commitment to strengthen regulatory requirements:

> […] we will review the government's ability to hold CNI operators to account to ensure they invest in the cyber security of critical systems and effectively manage their risk, including from their supply chains. We will strengthen the regulatory framework, to improve its coverage, powers, and agility to adapt, within the context of broader national security risk and rapidly changing threat and technology.[174]

In contrast to its stance on broader resilience standards, the Government also recognises that this work requires some urgency, committing to set "specific and ambitious cyber resilience targets" for all CNI sectors by 2025.[175] It commenced this workstream by consulting on changes to the NIS regulations, proposing to apply them to managed services (e.g. those outsourced to an external IT company, making up part of an operators' critical supply chain), allow Ministers to make changes to the regulations without primary legislation (to make them more responsive to the evolution of cyber threats), and improve cyber incident reporting to regulators.[176] The National Cyber Strategy also aims to increase the adoption of the NCSC's more stringent Cyber Assessment Framework among CNI operators, although it does not specify how it intends to achieve this outcome, nor what baseline data it is operating from.[177]

48. Clearly, new resilience standards will only have an impact if they are properly implemented and enforced, with robust oversight mechanisms. Unfortunately, there is strong evidence to suggest that this is not currently the case. The Government's second post-implementation review of the NIS regulations, published in July 2022, found that:

- 42% of (surveyed) operators of essential services indicated that "they do not have the skills and capacity to deliver their obligations under the NIS Regulations";

[171] NCC Group (RAN0012)

[172] Thales (RAN0019)

[173] Department for Science, Innovation and Technology, Cyber security breaches survey 2023, 19 April 2023

[174] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022

[175] Cabinet Office, National Cyber Strategy 2022 Annual Progress Report 2022–2023, 14 August 2023

[176] Department for Digital, Culture, Media and Sport, Government response to the call for views on proposals to improve the UK's cyber resilience, 30 November 2022

[177] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022

- "Competent authorities"—those responsible for enforcing the regulations, such as Ofgem, Ofcom and the Civil Aviation Authority—need "more resources to carry out what they deem to be an effective job of enforcing the Regulations";
- The lead Department (now the Department for Science, Innovation and Technology, or DSIT) "needs to conduct work to assess why the enforcement regime is not being utilised where it is merited"; and
- "Greater consistency in regulatory implementation across sectors is required, alongside the creation of performance metrics so that we can better measure the impact and effectiveness of the Regulations".[178]

In other words, there are major shortfalls in regulators' ability or willingness to implement existing resilience standards effectively, and CNI operators are unable to secure the right resources and skills. Some regulators pointed to "a lack of skills and experience to undertake the CAF framework across their sector", and to "difficulties in attracting and retaining sector-specific security skills".[179] This is exacerbated by cyber skills shortages across the UK economy, as we touch upon in Chapter 6. In the absence of a single regulator on cyber resilience, the National Cyber Strategy fails to identify how the new cyber resilience standards will be implemented or overseen.

49. **Unlike many areas of national resilience, the Government has imposed cyber resilience requirements on most CNI operators through the 2018 Network and Information System (NIS) regulations, and has also committed to imposing new cyber resilience standards on CNI by 2025. There are significant issues with the implementation and oversight of the existing regulations, however, linked to a lack of regulator capability and cyber skills. Plans to extend the NIS regulations to CNI supply chains need to be accompanied by further work to ensure that they can be implemented effectively.** ***The Government must scope the feasibility of establishing a cross-sector regulator on CNI cyber resilience to oversee the implementation of the NIS regulations, and to make recommendations for investment and legislative reform. The Government should report back to us on the outcome of this scoping work by March 2024.***

Exercising

50. Exercising is a core part of the Government's efforts to enhance the UK's resilience to a range of threats and hazards. Cabinet Office guidance describes an exercise as a "simulation of an emergency situation".[180] The 2022 Resilience Framework acknowledged that Government efforts in this space needed to be improved, with a commitment to "reinvigorate" the National Exercise Programme, to "bring together key partners to stress test our plans, structures and skills and embed lessons captured into our doctrine and standards".[181]

[178] HM Government, Second Post Implementation Review of the Network and Information Systems Regulations 2018, 4 July 2022

[179] HM Government, Second Post Implementation Review of the Network and Information Systems Regulations 2018, 4 July 2022

[180] Cabinet Office Guidance, Emergency planning and preparedness: exercises and training, 11 November 2014

[181] HM Government, The UK Government Resilience Framework, December 2022

51. We have previously called on the Government to enhance its exercising in other risk areas, including climate risks to CNI.[182] Witnesses also pointed to this as crucial for CNI operators, given that "it is not a case of 'if', but 'when' they will be subject to a cyber-attack".[183] More broadly, organisations "need to understand and rehearse these events", particularly "how they would recover from a truly catastrophic event",[184] noting that decision-making in the aftermath of an attack might be sub-optimal if an organisation had not properly rehearsed for such a scenario.[185] The NCC Group called for "more widespread adoption of realistic, intelligence-driven cyber security assurance testing", in which "ethical attack teams replicate the tactics, techniques and procedures of known threat actors", testing how the organisation would respond.[186]

52. The Government told us that it undertakes regular internal cyber exercising, "largely led at the departmental level and supported by the NCSC and NCCU [the National Cyber Crime Unit of the NCA]",[187] and the NCSC has recently introduced a new assurance scheme for companies offering cyber exercising services.[188] We understand the NCSC is also including ransomware in its exercising scenarios for the UK Industrial Control System (ICS) Cyber Lab project.[189] However, these schemes do not currently involve CNI operators which means that no central body is identifying systemic cross-sector risks, or rehearsing for an event that involves more than one CNI sector. Professor Creese emphasised the vital importance of considering cross-sector vulnerabilities during exercising, accounting for the significant interdependencies and co-dependencies between CNI sectors:

> "In single sectors and across multiple sectors, there are circles of dependency. The systemic risk could be because we use common technologies that suffer the same vulnerabilities, so somebody can attack us all at once with a single weapon. The simulations we have been running show that that is a pretty acute maximising worst-case outcome for a system, ecosystem or country, for example.
>
> There are very particular dependencies: co-dependence on energy source, co-dependence on communications provided by ICT infrastructure sources, dependence of transport or finance on energy et cetera. Pick any of your CNI sectors and you would be hard pressed to convince yourselves that there is not some kind of linkage between them."[190]

Jayan Perera, a cyber incident response expert for Control Risks, also called for the Government to focus more on "industry-wide exercising", looking at "the interconnections between systemically important industries".[191]

53. **We welcome the Government's efforts to reinvigorate the National Exercise Programme. The majority of UK CNI is run by private operators, however, so it is**

[182] JCNSS, Readiness for storms ahead? Critical national infrastructure in an age of climate change: First Report of Session 2022–23 (HC132/HL74), 27 October 2022

[183] Thales (RAN0019)

[184] Mr Andrew Jones (RAN0002)

[185] Q7 (Professor Sadie Creese)

[186] NCC Group (RAN0012)

[187] Cabinet Office (RAN0018) and Cabinet Office (RAN0040)

[188] NCSC blog post, New scheme ready for Cyber Incident Exercising providers, 26 September 2023

[189] Cabinet Office (RAN0040)

[190] Q7 (Professor Sadie Creese)

[191] Q11

vital that these companies are invited to participate in the Programme. The exercises should also consider broader impacts, beyond a single infrastructure sector. ***As part of the National Exercise Programme, the Government should hold regular national exercises to prepare for the impact of a major national ransomware attack affecting multiple CNI sectors, engaging CNI operators to stress-test their response and ensure a swift recovery. It should also ensure that the insights from these exercises are fed back to Lead Government Departments and regulators, so that they enhance preparations for future potential attacks.***

Local authority resilience

54. The services provided by UK local authorities are absolutely critical to the smooth-running of society and the wellbeing of the UK population, from child protection through to elderly care and environmental health. As a result, cyber-attacks on local authorities have the potential to impact significantly on the most vulnerable in society. This was demonstrated by a series of attacks over the last four years:

- As outlined in Chapter 1, Redcar & Cleveland Borough Council fell victim to a ransomware attack on its server estate in February 2020, which kept it offline for almost a week. The attack incapacitated key services and caused "catastrophic" data loss.[192]

- Hackney Council experienced a major ransomware attack in October 2020, which disrupted council services for months and cost the Council over £12 million,[193] through lost income and attempts to restore and strengthen its IT systems.[194] The attack—which came during the Covid-19 pandemic—locked the council out of key data and services, including information on benefit and council tax payments.[195] As of August this year, it still hadn't rebuilt its systems for housing services.[196]

- Although not a ransomware attack, Gloucester City Council has faced costs of around £800,000 after its systems were infected by malware from a Russian threat actor in December 2021, causing delays to benefits payments, property sales and planning applications.[197]

55. The 2022 Government Cyber Security Strategy (outlined in further detail in Chapter 5) largely leaves work on local government cyber resilience to the Department for Levelling Up, Housing and Communities (DLUHC), noting that the Lead Government Departments for each CNI sector are "best placed to understand the unique characteristics of the organisations within their purview".[198] Work is underway to strengthen Local Resilience Forums (which are responsible for planning for local emergencies), including through

[192] Computer Weekly, Redcar & Cleveland Council confirms ransomware attack, 27 February 2020

[193] *Hackney Citizen*, Cyber attack recovery effort cost Hackney Council over £12m last year, 13 October 2022

[194] Computer Weekly, Annual costs of Hackney ransomware attack exceed £12m, 14 October 2022

[195] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022

[196] *Inside Housing*, Hackney to procure new IT system after three years of struggle following 'devastating' cyberattack, 18 August 2023

[197] *Gloucestershire Live*, Gloucester cyber attack: A year since hackers disrupted vital services for thousands of citizens, 21 December 2022; Gloucestershire City Council (News), Investigation concludes into cyber-attack on Gloucester City Council, 7 June 2023

[198] HM Government, Government Cyber Security Strategy 2022–2030, 25 January 2022

piloting the role of a Lead Resilience Officer,[199] but LRFs have no specific responsibility for cyber resilience. The Spending Reviews of 2020 and 2021 announced a total of £85.8 million of funding to improve local authority cyber resilience,[200] but a quarter of surveyed council officials reported recently that they had made "no progress" on cyber security, and that their security systems remained "outdated".[201]

56. After the attack on Redcar and Cleveland Borough council, Cllr Lanigan told us that she had given talks to a number of councils to advise them not to integrate all their data onto one system,[202] after her Council been given a "clean bill of health" shortly prior to the attack. She noted that Redcar and Cleveland had "followed all government guidelines, and we did not think that we were at risk";[203] she suggested that the Government tends to "leave it to us through the LGA [Local Government Association]" to produce guidance on cyber resilience.[204] We asked the NCSC what more they were doing to ensure that local authorities were better defended against ransomware.

57. Despite "extensive work" on resilience, the LGA told us that ransomware risks to local authorities are still increasing, identifying it as the number one cyber security risk to councils. Vulnerabilities are caused by legacy IT and limited budgets, underinvestment in new technology, increased digitisation (expedited by the pandemic and remote working), supply chain risks, and the fact that councils share data systems with various agencies to deliver essential services.[205] One witness compared local authorities to "distressed debt companies": they "often feel the impact of ransomware the most because they have had a period of underinvestment", and do not have the staff to enable them to "recover in a timely fashion".[206] The LGA called for further Government investment in training and upgrading legacy IT, and for guidance from central Government on supply chain risks, noting that this work is "beyond the scope of any single council".[207] The NCSC Annual Review for 2023 reported that 73% of reports to the NCSC Vulnerability Reporting Service have come from Local Government and local services, whilst central government departments make up 21% of reports.[208] In correspondence with the Deputy Prime Minister, he stated that whilst security expectations have remained consistent since 2021, the nature of targets set for governments critical functions, including local authorities and how performance is measured against them, has changed.[209]

58. **Although we recognise the value of peer support, it should not have fallen to Redcar and Cleveland Council's Leader to train other councils how to prevent and respond to cyber-attacks, following their own devastating attack in 2020. Local authorities are on the frontline of support for the most vulnerable in society. The Government needs to provide much more active support. This should include how to prevent and respond to major cyber-attacks, recognising the extremely challenging financial circumstances in which they operate. The Government's understanding and expectations regarding local authority preparedness has developed since 2021. However the problem persists, the**

[199] HM Government, The UK Government Resilience Framework, December 2022
[200] HM Government, Autumn Budget and Spending Review 2021 (HC822), 27 October 2021
[201] *Cities Today*, Majority of UK councils say their cybersecurity is outdated, 9 May 2023
[202] Q19 (Councillor Mary Lanigan)
[203] Q15 (Councillor Mary Lanigan)
[204] Q23
[205] Local Government Association (RAN0024)
[206] Q11 (Ollie Whitehouse)
[207] Local Government Association (RAN0024)
[208] NCSC, Annual Review 2023, p61
[209] Cabinet Office (RAN0042)

NCSC Annual Review for 2023 reported that 73% of reports to the NCSC Vulnerability Reporting Service have come from Local Government and local services. We recognise and welcome the work undertaken by the NCSC so far, but urge the Government to pursue a more focused effort which proactively seeks to support local government with preventative support and strengthened resilience measures. *The NCSC should be funded to establish an enhanced and dedicated local authority cyber resilience programme, including intensive support for local exercising and on securing council supply chains.*

4 Responding to attacks—victim support and recovery

59. The impact of cybercrime on its direct victims, including financial loss, psychological harm and ill health,[210] has been well documented. Ransomware has unique characteristics, however, so we sought to understand the true nature of the UK victim experience and their access to adequate support. Such support might be provided by:

- **The NCSC**, the UK's national technical authority for cyber security, which may provide direct support to certain significant victims (e.g. CNI operators), and which offers a list of assured cyber incident response (CIR) companies through its CIR scheme.[211]

- **The NCA**, which leads the UK's fight against serious and organised crime. The NCA's National Cyber Crime Unit (NCCU) leads its work to disrupt and respond to ransomware, including through its Triage, Incident Coordination and Tasking Team (TICAT), which provides an operational response for critical incidents.[212]

- **Police forces**: the NCCU may 'task' the National Cyber Crime Network (including the Regional Cyber Crime Units) with incidents that are not considered to require a national-level response.[213] The Network also comprises Local Cyber Crime Units in all 43 forces in England and Wales.[214]

- Private sector **CIR companies**, to which victims may turn for support with incident management, negotiation with threat actors and recovery.

- For some insured victims, **professional services** support through an **insurance panel**—this might include legal advice, PR consultancy, business support and CIR support.[215]

This chapter considers our findings on UK victims' experiences, access to cyber insurance, and issues linked to the reporting of attacks and the payment of ransoms.

The UK victim experience

60. We encountered major obstacles when trying to take formal oral evidence from ransomware victims, reflecting a general reluctance to report incidents publicly,[216] so we held a private roundtable event in May. Key themes from that event are outlined in Box 2. They include the significant impact of the attack on the primary victim, the fact

[210] For example: Button, S., Shepherd, D., Wang, V., Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective, *Criminology and Criminal Justice*, October 2022

[211] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022

[212] Cabinet Office (RAN0018)

[213] Cabinet Office (RAN0018)

[214] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022

[215] For example: RSA Insurance website, Cyber insurance, accessed 6 October 2023

[216] FTI Consulting LLP, Clifford Chance LLP (RAN0034)

that mitigations and resilience measures—some quite advanced—had not succeeded in preventing the attack, the major challenges involved in recovering from the incident, and the lack of Government support.

61. These findings were reflected in much of the oral and written evidence that we received. Submissions also emphasised:

- **The significant impact of attacks on primary** *and* **secondary victims.**[217] When public services have been attacked, patients have faced delays to their care on top of existing Covid backlogs, and children's services have been put at risk.[218] In many attacks, "a chain of secondary and tertiary victims […] find themselves hit with a wall of silence from the primary victim", and can be left feeling particularly anxious.[219] According to one witness, secondary victims are sometimes only notified about an attack after their sensitive information has been leaked on the dark web.[220] Primary victims have found themselves locked out of digital systems and forced to resort to pen and paper (one witness described this as going "back to a pre-computer era of the 1950s in mere minutes"),[221] and have faced significant recovery costs,[222] complex legal and regulatory challenges,[223] and long recovery times—up to a year for some organisations.[224]

- **The lack of state support for most victims of ransomware, particularly SMEs** and other organisations not considered CNI operators.[225] Witnesses asserted that support is only provided by the NCA and the NCSC in the "most serious cases", and that it is "not resourced to respond adequately to incidents occurring outside of CNI".[226] Jayan Perera confirmed that SMEs "find it much harder to get hold of people to support them" and are "often left to their own devices";[227] he argued that "We need to start getting more support for victims in some way, shape or form".[228] Others claimed that the state response is "little to non-existent across the board",[229] and that this "risks breeding apathy or even a loss of trust among victims in the ability of government and law enforcement to protect them".[230] Even some 'CNI-adjacent' services that retain data on vulnerable groups—such as schools and academy chains—have little access to NCSC or law enforcement support.[231]

- **The poor understanding of ransomware among local police forces**: according to one witness, the responding police force is "usually unfamiliar with cyber incidents and ransomware, and/or takes a significant amount of time to

[217] Q9 (Jayan Perera)
[218] Q17 (Cllr Mary Lanigan and John Ward)
[219] JUMPSEC (RAN0009)
[220] JUMPSEC (RAN0009)
[221] For example: Q15 (Cllr Mary Lanigan and John Ward), Mr Andrew Jones (RAN0002)
[222] For example: Q15 (Cllr Mary Lanigan)
[223] For example: Mr Andrew Jones (RAN0002)
[224] Q34 (Sarah Stephens)
[225] Q44 (Aidan Larkin), Royal United Services Institute (RAN0032)
[226] FTI Consulting LLP, Clifford Chance LLP (RAN0034)
[227] Q7
[228] Q14 (Jayan Perera)
[229] Q44 (Aidan Larkin)
[230] Royal United Services Institute (RAN0032)
[231] Royal United Services Institute (RAN0032)

investigate an incident".[232] In some cases, "a local police officer turns up at the door of a small business in the middle of an incident offering to help", but is then "unable to offer any meaningful assistance".[233] We were told that Local Cyber Crime Units "play an important role in supporting victims", but "many do not have the skills nor resources needed to provide a full-scale service".[234]

- As a result of this lacuna, the fact that **many victims have to turn to private cyber incident response firms**. Even Redcar and Cleveland Council told us that they had to call on "private security" for the first week after they were attacked, before the NCSC stepped in.[235] RUSI argued that ransomware response and recovery has, in effect, been "privatised" by the Government for most victims,[236] and others noted that victims are forced to turn to the private sector due to lack of state support.[237] The NCSC actively encourages them to do so, providing a list of approved CIR companies,[238] but witnesses told us that SMEs are "not the target clients for these very established CIR companies",[239] and are left with "limited guidance on how to identify and procure reliable and affordable providers".[240]

- **The need for organisations to focus more on mitigating rather than preventing attacks**, due to the sophistication of threat actors: one victim noted that "an assumption should be made that technology will ultimately fail to stop these attacks", and "attention should [therefore] be redirected to establishing true resilience in core systems and on being well versed in recovery procedures".[241]

[232] FTI Consulting LLP, Clifford Chance LLP (RAN0034)
[233] Q22 (Sarah Stephens)
[234] NCC Group (RAN0012)
[235] Q18 (Cllr Mary Lanigan)
[236] Royal United Services Institute (RAN0032)
[237] For example: FTI Consulting LLP, Clifford Chance LLP (RAN0034)
[238] JUMPSEC (RAN0009)
[239] JUMPSEC (RAN0009)
[240] Royal United Services Institute (RAN0032)
[241] Mr Andrew Jones (RAN0002)

Box 2: Our ransomware victims' roundtable

In May 2023, we held a private roundtable event with representatives of seven organisations that had experienced ransomware attacks. The following key themes and findings emerged:

- The impact of the attacks on all the participants' organisations was significant. One participant noted that they had multiple back-ups, but the attackers had deleted their virtual infrastructure so they had to rebuild it from scratch, which severely disrupted their operations.

- Most participants had prepared in some way for an attack, sometimes through more generic business resilience/critical incident exercising or protocols, or through crisis management training for relevant staff.

- Even those who had extensive mitigations in place could not defend against all permutations of a ransomware attack. If they had imposed such mitigations, the business would not have been able to function properly, because it would have been so locked down. As a result, one participant's organisation was focusing additionally on recovery exercising, to avoid being shut down by its regulator in the event of a major attack.

- Recovery for most participants had been extremely challenging. One said that they were two-and-a-half years past the attack and still not fully recovered, having made the decision to rebuild their systems from scratch. Others said that it took months to recover properly, even if they were up and running again within weeks.

- The attacks took a heavy toll on staff: one participant spoke of working for two and a half months without a day off, with meetings at 8.30am, 6pm and 10pm every day. Another said that it was an "emotional thing, you feel like a victim", made worse by the fact that they could not talk about it because it was "seen as a shameful thing". They had to write the messages to the threat actor as part of their negotiation without support, and said it could be a "lonely place to be".

- Law enforcement communication was generally described as a one-way street, without much information shared in return. One participant (a CNI operator) had a good response from the NCA and NCSC, with a lot of support provided. Several participants had relevant cyber insurance and gained access to support through their insurer, which one described as "lots of hand holding". Others used specialist law firms to navigate their response.

- The importance of having insurance was emphasised, but one participant reported that it had taken two years to return to a reasonable premium after the attack. They had faced an immediate increase of 50%.

- Several participants had paid the ransom, and most of those who paid had their data unlocked or returned. One described their decision to pay as one of the hardest they had ever made: they did so with a "heavy heart".

62. Though its written evidence made very little reference to victim support, the Government has shown some recognition of the broader shortfalls in its response to cybercrime victims. Its National Cyber Strategy aims to ensure, by 2025, that it is "easier to report cyber incidents and victims of cyber crime receive better support".[242] Its Fraud Strategy further commits to "tailored support to victims at a local level across the whole of

[242] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022

England and Wales", through the National Economic Crime Victim Care Unit. When the Minister was asked about victim support on the 15 November, he said the Government were "looking at ways" to encourage reporting and "incentivise best practice".[243]

63. NCA witnesses described the state response to ransomware as a "complex picture". They acknowledged that, "Over the years, the [police] response locally has not been as good as it should have been", but noted that the 43 forces are not expected to have specific ransomware capabilities.[244] Graeme Biggar told us that attacks reported as a crime (rather than as a data breach) would come to the NCA,[245] but Rob Jones subsequently pointed to private sector support, noting that organisations reporting to the NCSC would "get access to a good CIR company and the ability to mitigate that attack".[246] Graeme Biggar added:

> Could we get better in helping local authorities or SMEs when they are attacked? Absolutely, but, as we know from the Gloucester [City Council] experience and lots of others, once you have been attacked it is a long, hard road to recovery and it is expensive.[247]

64. The NCSC's Annual Review 2023 commented on the potential risks of attacks in the run up to an election. The review said that the UK Government "is almost certain that Russian actors sought to interfere in the 2019 general elections". For this reason, the review said that with UK and US elections on the horizon "we can expect to see the integrity of our systems tested again".[248] The Review acknowledges the role and risks posed to high-risk individuals and defending our values. The NCSC said it had launched a new 'opt in service' which allows the NCSC to alert high-risk individuals of malicious activity on their personal devices or accounts and to provide advice.[249] In correspondence sent to the committee on 30 November 2023, NCSC said that "Russia-based and Iran-based actors continue to conduct spear-phishing campaigns against politicians, journalists, activists and other groups". The NCSC provided some reassurances that their offer of support had been "expanded". However, the NCSC only referred specifically to the offer of "personal support" for "candidates and Returning Officers ahead of the General and Mayor Elections" making no commitment to support political parties as a whole or commitments to public information campaigns on the topic. The Deputy Prime Minister did not confirm whether additional funding had been secured to provide this assistance.[250] We return to the law enforcement response to ransomware in Chapter 6.

65. **Many ransomware victims feel there is insufficient support from law enforcement or Government agencies, with limited state resources focused on the most critical organisations. For smaller organisations and those falling outside the boundaries of critical national infrastructure, the NCSC's post-incident support appears limited to a list of approved cyber incident response companies, which may be beyond the financial reach of many victims. These gaps in support apply to important elements of the public sector too, including schools and colleges, and stand in stark contrast to victim support for comparable thefts or ransom demands in the offline world.** ***The***

[243] Q80
[244] Q57
[245] Q57
[246] Q57
[247] Q57
[248] NCSC, Annual Review 2023, 14 November 2023, p20
[249] Q78
[250] UK Government (RAN0042)

NCSC and NCA should be funded to provide negotiation, recovery and remediation capabilities to all public sector victims of ransomware, to the point of full recovery. The NCSC should also explore, with the cyber incident response industry, the possibility of establishing a 'pro bono', industry-led scheme for charities and small businesses, akin to those provided by many major law firms.

66. **The emphasis on supporting high-risk individuals and protecting electoral integrity is undoubtedly welcomed. We would, however, welcome a more direct approach from the NCSC in their offer of support to political parties and high-risk individuals. It is unclear if the support for 'high risk individuals' will be offered to all parties before, during, and after an election and what work the NCSC is doing to preserve the integrity of free and fair elections in the UK overall. This work is vital to defending democracy and providing impartial support.** ***Our committee therefore requests a private briefing on the preparation that is being put together for an upcoming election and how this support will be provided and delivered.***

Insurance

67. As outlined in Box 2, we heard from a number of victims who accessed vital support through their insurer, and spoke highly of the benefits of cyber insurance. RUSI and other witnesses noted that insurance can make a substantial difference to ransomware victims, particularly SMEs, providing both specialist advice and recovery funds.[251] Insurance also has the potential to drive up cyber security standards, by linking cyber resilience to the cost and availability of coverage.[252]

68. Unfortunately, the UK cyber insurance market is in an extremely poor state,[253] with "demand outstripping capacity and insurers raising premiums and setting tougher conditions for coverage".[254] One insurer told us that 90% of their clients had seen their premiums increase during the third quarter of 2022, on average by 50%. This came on top of a 70% increase during the previous year.[255] According to the LGA, premiums for local authorities are so high that many council leaders prefer to spend their limited funds on cyber resilience measures instead.[256] Cllr Lanigan confirmed that the cost for Redcar & Cleveland Council to insure against ransomware attacks would have been "astronomical".[257] This so-called 'hardening' of the market has been attributed to:

- A sudden spike in claims in 2018 and 2019 as the ransomware threat "started to explode", linked to the increasing prevalence of ransomware-as-a-service,[258] which in turn led to "eye-watering losses" for some insurers.[259]

[251] Royal United Services Institute (RAN0032), Q24 (Sarah Stephens), Dr Gareth Mott (Lecturer at Institute of Cyber Security for Society (iCSS), University of Kent); Sarah Turner (PhD Researcher at Institute of Cyber Security for Society (iCSS), University of Kent); Dr Jason Nurse (Senior Lecturer at Institute of Cyber Security for Society (iCSS), University of Kent) (RAN0031)

[252] RUSI Occasional Paper (Jamie MacColl, James Sullivan, Jason R C Nurse, Sarah Turner, Gareth Mott, Edward Cartwright and Anna Cartwright), Cyber Insurance and the Ransomware Challenge, 2023

[253] FTI Consulting LLP, Clifford Chance LLP (RAN0034)

[254] Royal United Services Institute (RAN0032)

[255] Q27 (Sarah Stephens)

[256] Local Government Association (RAN0024)

[257] Q15

[258] Q27 (Sarah Stephens)

[259] Royal United Services Institute (RAN0032)

- The increasing sophistication and severity of cyber-attacks, and their links to geopolitical conflicts.[260]

- Increasing diligence standards in insurance provision, meaning that coverage is "increasingly limited to organisations that are already relatively sophisticated in their security posture",[261] with particularly prohibitive conditions for some sectors.[262] This is exacerbated by "data scarcity" about attacks, which means that underwriters lack evidence on which to base their risk assessments and quotations.[263]

- Concerns around the sensitivity of the data held by public sector clients, and associated liabilities.[264]

69. The Government had acknowledged that the cyber insurance market is "underdeveloped", and told us that the NCSC has assembled an "Insurance Trust Group" in a bid to improve relations with the industry.[265] Witnesses also acknowledged that there has been some collaboration between the Government and insurers, but called for more to be done,[266] and the insurance industry[267] argued for "greater levels of Government intervention and investment".[268]

70. We asked the Deputy Prime Minister to consider alternative models of Government support or intervention, such as a Government-backed reinsurance scheme (see Box 3 for further details). He responded that it would "not be an appropriate use of public funds", and that the Government's "principal position" is to avoid assuming liability for risks "where the market could feasibly perform this function".[269] He did not address how a healthier market might emerge, given its current state. Nor did his response acknowledge that the Flood Re model—outlined below—is entirely self-funded, and does not offer an unlimited Government guarantee. When asked further about the scope of a Flood Re model for cyber insurance, the Minister of Security said: "The reality is that the market is addressing quite a lot of these questions pretty effectively at the moment."[270] He specified that this included protection that small businesses may need.

71. Sarah Stephens, Head of Cyber at Marsh Speciality, an insurance risk broker, said that Marsh would be "supportive of a well-constructed government cyber reinsurance or back-stop mechanism", suggesting that it should be precisely targeted to the aspects of cyber risk that private markets consider to be uninsurable.[271]

[260] FTI Consulting LLP, Clifford Chance LLP (RAN0034), Association of British Insurers (RAN0021)
[261] FTI Consulting LLP, Clifford Chance LLP (RAN0034)
[262] Dr Gareth Mott (Lecturer at Institute of Cyber Security for Society (iCSS), University of Kent); Sarah Turner (PhD Researcher at Institute of Cyber Security for Society (iCSS), University of Kent); Dr Jason Nurse (Senior Lecturer at Institute of Cyber Security for Society (iCSS), University of Kent) (RAN0031)
[263] Royal United Services Institute (RAN0032), Association of British Insurers (RAN0021)
[264] Q24 (Sarah Stephens)
[265] Cabinet Office (RAN0018)
[266] Royal United Services Institute (RAN0032)
[267] Association of British Insurers (ABI) and International Underwriting Association of London (IAU) (RAN0021)
[268] Association of British Insurers (RAN0021)
[269] Correspondence from the Deputy Prime Minister to the JCNSS Chair, 10 July 2023
[270] Q79
[271] Q30

Box 3: Government-guaranteed insurance

When risks have been considered too significant or too uncertain for the market to provide adequate insurance cover, the Government has previously 're-insured' the risks taken on by private insurers.[272] There are two significant examples of Government-guaranteed insurance:

- **Pool Re** is the longest-established Government-guaranteed reinsurance scheme, and was set up to stabilise the market for terrorism insurance for private properties, following a spate of IRA bombings in the early 1990s. Premiums paid by insurers to Pool Re are invested into pooled reserves that could be drawn upon in the event of a terrorist attack (including some terrorist cyber-attacks, if they result in physical damage).[273] Around half the premiums and some investment returns are paid to HM Treasury, which gives an unlimited guarantee of additional funding for pay-outs after a terrorist attack, if ever required. The build-up of reserves means that Pool Re would have to reach £11 billion of losses before needing to call on the Government guarantee, which has never yet been invoked.[274]

- **Flood Re** was established following major UK flooding in 2012, after which some homes became uninsurable. A Government levy on the insurance sector funds a government-backed reinsurance scheme, allowing insurers to offer lower premiums than would otherwise be unviable for high-risk homes. The scheme effectively runs an underwriting loss, but is funded by a levy on all UK household insurers.[275] The Government's backing is not unlimited, as for Pool Re, but is topped up with an 'outwards reinsurance programme' to protect Flood Re up to a liability limit of £2.28 billion.[276] Flood Re has resulted in a vast increase in insurance availability for householders who have previously made flood claims, along with significant price reductions for that insurance.[277]

72. **Cyber insurance can provide a vital lifeline for ransomware victims, offering the sort of support and technical advice not offered by state agencies, as well as driving up cyber security standards through conditions of coverage. Unfortunately, there remains a woeful lack of UK coverage: premiums are unaffordable for many organisations, and have increased drastically in recent years. There are precedents for more extensive Government interventions, where market failures in insurance have wider societal implications. Given the losses endured by ransomware victims and the costs to businesses and public finances, there is a strong economic case for the Government to do more.** ***The Government should work with the insurance sector to establish a re-insurance scheme for major cyber-attacks, akin to Flood Re, to ensure the sustainability and accessibility of the market.***

Reporting

73. Most of the victims who took part in our roundtable had reported their attack to law enforcement, but this is not the norm. The Government's written evidence noted that only

[272] Office for Budget Responsibility website, Government-guaranteed insurance against systemic risk (Pool Re), accessed 28 September 2023

[273] Office for Budget Responsibility website, Government-guaranteed insurance against systemic risk (Pool Re), accessed 28 September 2023

[274] Office for Budget Responsibility website, Government-guaranteed insurance against systemic risk (Pool Re), accessed 28 September 2023

[275] Flood Re website, Common FAQs, accessed 28 September 2023

[276] Flood Re Annual Report, year ended March 2023

[277] Department for Environment, Food and Rural Affairs, Amendments to the Flood Re Scheme: Consultation, February 2021

2–10% of cybercrimes come to the attention of law enforcement[278] (although the NCA suggested that ransomware would be "at the high end of that")[279]. Victims are required to report an attack to the Information Commissioner's Office (ICO) under certain conditions[280] but not to law enforcement (although the ICO may notify law enforcement and/or regulators in some circumstances).[281] We heard that the current commercial and regulatory climate may disincentivise victims to report, given the reputational ramifications,[282] and many choose to focus instead on their recovery.[283]

74. We received overwhelming evidence on the challenges created by the lack of authoritative data on ransomware, and even the Government acknowledged that low reporting levels present a "challenge when exploring policy options to combat this threat".[284] Other witnesses argued that the lack of data:

- Hampers the law enforcement response:[285] as US National Cyber Director Chris Inglis recently commented, "to properly address risk, we have to first understand it";[286]
- Deprives other organisations of the opportunity to learn lessons from ransomware victims[287] and prevents "broader society" from benefiting from a potential "catalogue of learnings",[288] including the ability to understand the effectiveness of different risk control practices;[289] and
- Creates challenges for insurers, who have called for more transparency about the size and scope of incidents.[290]

75. The NCA's Graeme Biggar showed little enthusiasm for the prospect of mandatory reporting, noting that he could recall no other crimes in which "you are required, by law, to report that you have been a victim". He suggested instead that insurance companies could require victims to obtain a police report.[291] Others have argued that businesses should be encouraged or compelled to report to an independent body,[292] however, and the US Senate has passed legislation requiring CNI organisations to report hacks and ransomware attacks.[293,294] The US Cyber Security Strategy asserts that these notifications will "improve efforts to identify the root causes of incidents" and "improve decision-

[278] Cabinet Office (RAN0018)
[279] Q62 (Rob Jones)
[280] ICO website, Report a breach, accessed 28 September 2023
[281] ICO website, Report a breach, accessed 28 September 2023
[282] Royal United Services Institute (RAN0032)
[283] FTI Consulting LLP, Clifford Chance LLP (RAN0034)
[284] Cabinet Office (RAN0018)
[285] Q62 (Graeme Biggar)
[286] Atlantic Council, National Cyber Director Chris Inglis: We need to become a 'harder target' for our adversaries, 4 August 2021
[287] Royal United Services Institute (RAN0032), Secureworks (RAN0036)
[288] PwC UK (RAN0006)
[289] Q9 (Professor Sadie Creese)
[290] Q30 (Sarah Stephens)
[291] Q62 (Graeme Biggar)
[292] For example: *Raconteur*, Is legislation the best defence against ransomware attacks? 2 May 2023
[293] These will come into force once the Cybersecurity and Infrastructure Security Agency (CISA) has fully clarified requirements. From: *Security Intelligence*, What CISOs should know about CIRCIA incident reporting, 8 December 2022
[294] Cabinet Office (RAN0018)

making within government on how to respond".[295] John P. Carlin also noted the potential for the legislation to implicate software companies that need to do more to secure their networks against ransomware,[296] through greater levels of transparency.

76. **Victims are currently disincentivised to report ransomware attacks, making it difficult to understand fully the nature and scale of the threat, and how best to tackle it. The Director General of the NCA has suggested that it would be unusual for the Government to require any victim of crime to report an attack—but there are usually greater incentives for reporting of serious crime to take place. The US has also recognised this unique challenge, legislating to mandate reporting by CNI operators. The Government acknowledges that this lack of data creates challenges for the policy response, and experts have told us that it reduces their understanding of how best to protect other organisations against future attacks.** ***The Government should urgently establish a central reporting mechanism for ransomware attacks, and consider whether to require all UK organisations to report an attack within three months. As part of reporting arrangements, the Government should specify that companies disclose:***

a) ***Which systems or data have been compromised;***

b) ***The identity and tactics of the attackers, if known;***

c) ***Technical details, such as the performance of security and operational systems whilst under attack;***

d) ***Key details on how the organisation has responded, including communication with secondary victims; and***

e) ***Which regulators have been notified.***

The data should be kept securely and used for threat intelligence, disruption and prevention work. It could also contribute towards a quarterly, anonymised public report on key ransomware trends.

Ransom payments

> If you receive a blackmail letter, prevent further handling of the letter and its envelope as soon as you recognise what it is. It contains evidence! If you need to handle it, use gloves and put it into a big paper envelope without folding it. Note when and how it arrived and who touched it.[297]

Guidance on hostage-taking, extortion and kidnapping, published on the NCA website.

77. Many victims of ransomware face a moral dilemma. They can choose either to pay the ransom in the hope of regaining control of their data and systems, or to resist paying money to criminals and risk having to rebuild their systems from scratch, or finding sensitive data leaked or sold on the dark web. Threat actors' increasing use of double or triple extortion means that back-ups may be insufficient to prevent damage, if data has

[295] The White House, National Cybersecurity Strategy, 2 March 2023, p.12

[296] John P. Carlin (Partner, Cybersecurity & Data Protection practice at Paul, Weiss, Rifkind, Wharton & Garrison LLP) (RAN0038)

[297] The European Network of Advisory Teams (EUNAT), Prevention and Coping Strategies: Kidnapping, Hostage Taking, Extortion, Attacks, published on the NCA website, accessed 9 September 2023

been exfiltrated and could be leaked or sold.[298] Many victims are also making this difficult choice (and are left to negotiate with the attacker) in the absence of any professional support.[299]

78. Although some countries are considering a ban on ransom payments,[300] the Government's official position remains that the decision is "ultimately a matter for the individual or organisations concerned".[301] Many witnesses warned against a ban, arguing it would create more shame and silence around cyber incidents.[302] The NCA agreed, noting that "we do not want people to pay ransoms and we will never advise people to do so", but arguing that a ban on ransoms would criminalise "the wrong part of the equation" and would 'double down' on the impact on victims. They also acknowledged that a ransom payment can sometimes be "the only way out", and the "lowest harm resolution to the incident".[303]

79. We heard that there is, nevertheless, scope for the UK authorities to do more to support victims through this difficult process.[304] RUSI said that there was "a vacuum of assurance and advice on best practices for ransom negotiations and payments",[305] and one witness compared the NCSC's approach unfavourably with the more mature, risk-based framework for health and safety, with the HSE producing regular guidance on "almost every aspect of Health and Safety on a regular basis".[306] The NCSC's advice on ransomware is detailed and wide ranging, but its main resource on what to do *after* a ransomware infection occurs is a 'joint advisory' with the cyber authorities of four other countries,[307] which contains highly technical advice on responding to malicious activity[308]—unlike the advice available for more 'traditional' blackmail and hostage taking, quoted above. The NCSC offers no public advice on negotiating with threat actors.

80. **While the Government maintains that UK victims should not pay ransoms, it is the only viable option for many of those directly affected, enabling them to keep their businesses afloat and prevent damaging leaks of personal data. Too many organisational leaders are left to face this moral dilemma alone, without any state intervention.** ***The NCSC must produce more detailed guidance—accessible to a non-technical audience—on how best to avoid the payment of ransoms after an attack, including negotiating techniques and sources of support for smaller organisations.***

[298] techUK (RAN0023)

[299] Royal United Services Institute (RAN0032)

[300] Including Australia - from *TechSpot*, Australia is considering a ban on ransom payments to hackers, 16 November 2022

[301] Cabinet Office (RAN0018)

[302] For example: Q34 (John Ward), JUMPSEC (RAN0009)

[303] Q63

[304] Royal United Services Institute (RAN0032), FTI Consulting LLP, Clifford Chance LLP (RAN0034)

[305] RUSI Occasional Paper (Jamie MacColl, James Sullivan, Jason R C Nurse, Sarah Turner, Gareth Mott, Edward Cartwright and Anna Cartwright), Cyber Insurance and the Ransomware Challenge, 2023

[306] FTI Consulting LLP, Clifford Chance LLP (RAN0034)

[307] Australia, Canada, New Zealand and the US (the Five Eyes partners)

[308] Cybersecurity and Infrastructure Security Agency (CISA) website, Cybersecurity Advisory: Technical Approaches to Uncovering and Remediating Malicious Activity (AA20–245A), Last revised 24 September 2020, accessed 26 September 2023

5 The strategic response—the Government's structures and approach

81. On 7 May 2021, the US company Colonial Pipeline was forced to shut down one of the country's largest and most vital oil lines for six days after a ransomware attack by Russian DarkSide operators, which affected its billing and accounting systems.[309] The shutdown affected 17 US States;[310] it led to a spike in fuel prices, panic buying, localised fuel shortages,[311] and the re-routing of some domestic and international flights.[312] President Biden declared a national state of emergency on 9 May. According to *The New York Times*, a confidential assessment by the Energy and Homeland Security Departments found that the US could only afford another three to five days with the Colonial Pipeline shut down before "buses and other mass transit would have to limit operations because of a lack of diesel fuel".[313]

82. The Colonial Pipeline attack moved ransomware firmly up the political agenda in the US: John P. Carlin told us that it "supercharged US efforts", leading to the creation of the international taskforce on ransomware, and to stricter regulatory requirements.[314] It also "focused the American public", by showing that a "not particularly sophisticated attack, which did not actually succeed in disrupting critical infrastructure, could still have the impact of causing lines at gas stations". It had an "immediate, tangible impact on people's lives".[315]

83. The UK is yet to experience an attack on the scale of Colonial Pipeline. The NCA confirmed that no attack has yet been categorised as "C1" for its operational response—the most severe category.[316] Perhaps as a result, some have argued that ransomware is not yet a political priority, as we outline in further detail below. This chapter considers the merits of those arguments and outlines the effectiveness of the Government's overall strategic approach to ransomware and to cyber security more broadly, including the delivery of key strategies, Ministerial oversight and political prioritisation.

Delivery of counter-ransomware policy and strategy

84. The Government has no public strategy on ransomware, although Rob Jones referred to a "coherent ransomware strategy" when he gave evidence to us in June, suggesting that it might exist in a confidential form.[317] The Government's response to ransomware is also delivered through a number of closely-related strategies, which are summarised in Box 4. The most relevant of these is the 2022 National Cyber Strategy, particularly its second pillar on Cyber Resilience—referenced in Chapter 3—and its fifth pillar on Countering Threats, which covers the detection and disruption of cyber-attacks.

[309] *Tech Target*, Colonial Pipeline hack explained: Everything you need to know, 26 April 2022
[310] *The Guardian*, US invokes emergency powers after cyber-attack on fuel pipeline, 10 May 2021
[311] *Reuters*, One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators, 9 June 2021
[312] *Flight Global*, Full impact of US pipeline shutdown still unclear, American reroutes two flights, 11 May 2021
[313] *New York Times*, Pipeline Attack Yields Urgent Lessons about US Cybersecurity, 14 May 2021
[314] Q48
[315] Q48 (John P. Carlin)
[316] Q66
[317] Q54

Box 4: Key government strategies and policy frameworks

A number of recent Government strategies are relevant to its response to ransomware:

- The 2022 **National Cyber Strategy**: unlike previous National Cyber **Security** Strategies, this has more wide-ranging aims linked to the UK's cyber 'eco-system', such as industrial capabilities and UK global leadership on cyber.[318] It sets out objectives to 2030, with the "vision" that the UK will "continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace in support of national goals". In line with the 2021 Integrated Review (IR), one of its five pillars focuses on "detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace". Commitments include a shift towards more "integrated and sustained" campaigns to "impose costs on our adversaries, pursue and disrupt perpetrators and deter future attacks". This is underpinned by the "continued development" and "scale-up" of the National Cyber Force, a defence-intelligence partnership intended to counter the UK's cyber adversaries, along with "new investment to enable law enforcement to pursue investigations at scale and pace", and "a major step up in data sharing across government and industry".

- As touched upon in Chapter 3, the 2022 **Government Cyber Security Strategy** focuses on protecting "core government functions" from cyber threats. Key actions include the establishment of a new Government Cyber Coordination Centre (GCCC), to "transform how data and cyber intelligence is shared"; a new vulnerability reporting service, allowing security experts and members of the public to report weaknesses in digital services; and investment in local authorities' cyber resilience.[319]

- The 2023 **Integrated Review Refresh** (IRR): this update to the 2021 IR sets out the Government's ambition to achieve a new "operating model" for security, described as achieving "security through resilience" (rather than security *and* resilience, as in the IR). This will involve much greater emphasis on pre-emptive protection and preparatory activity. 'Cyber security and resilience' is one of the IRR's five priority areas of vulnerability that require improved resilience, through which it mainly commits to "keep advancing" the 2022 National Cyber Strategy.[320]

- The 2023 **Fraud Strategy**, which includes £400 million investment in law enforcement to tackle economic crime over the next three years, a new National Fraud Squad with 400 new specialist investigators, and improved services for victims of fraud.[321]

85. There has been very little recent scrutiny of the Government's delivery against these strategies. The National Audit Office (NAO), responsible for auditing public spending, uncovered some concerning weaknesses in the delivery of the last National Cyber Security Strategy, outlined in Box 5 below. Some of these findings seemed to vindicate the concerns of our predecessor Committee, whose 2018 report on the cyber security of the UK's CNI found that the 2016–21 National Cyber Security Strategy lacked a clearly defined starting point, a clearly defined end point, and any metrics by which progress could be objectively assessed against a set timeframe.[322]

[318] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022

[319] HM Government, Government Cyber Security Strategy 2022–2030, 25 January 2022

[320] HM Government, Integrated Review Refresh 2023: Responding to a more contested and volatile world (CP 811), March 2023

[321] HM Government, Fraud Strategy: Stopping Scams and Protecting the Public (CP 839), May 2023

[322] JCNSS, Cyber Security of the UK's Critical National Infrastructure: Third Report of Session 2017–19 (HC222/HL1708), 12 November 2018

86. The 2022 National Cyber Strategy (NCS) seems to recognise that a more robust approach to governance and oversight is required. It is being delivered through a combination of departmental activity and the National Cyber Programme,[323] with governance provided by a "continuously evolving performance framework that reports to senior responsible officials and the National Security Council".[324] A recent NCS Annual Progress Report, published in August 2023, gave some further details on this Performance Framework. It includes:

- An "outcome profile" for each strategy outcome, which enables departments to clarify governance, sub outcomes, activities, policies, external factors, metrics and targets;
- A data-driven reporting template for pillars and outcome owners, who are required to complete it every six months;
- A performance scorecard with "a mixture of objective evidence and professional judgement" to determine a 'RAG rating'[325] status for each outcome; and
- A cross-strategy performance dashboard to visualise the evidence for "senior audiences" and summarise performance returns into a "succinct 10-page digital format".

The Progress Report also sets out plans to make further progress against the NCS objectives over the coming year, including by "announcing further steps on our policy response to ransomware".[326]

Box 5: The NAO's 2019 report on the National Cyber Security Programme

The National Audit Office last considered the Government's delivery against its cyber security objectives in 2019, when it reviewed progress in implementing the 2016–21 National Cyber Security Programme (the main vehicle for delivering the then National Cyber Security Strategy).[327] It concluded that the Programme had reduced the UK's vulnerability to cyber-attacks, but that:

- The Cabinet Office was only on track to deliver on three of the Programme's 12 objectives by 2021, and the Department had "high confidence" that it would meet only *one* of those objectives by 2021;
- Programme management weaknesses were "likely to continue to hamper delivery of the Programme and consequently the Strategy" up to 2021; and
- With the Strategy it was then preparing for 2021 (the National Cyber Strategy), the Department risked "repeating previous mistakes", in part because it was "unlikely that the Department will have decided on its future approach to cyber security in time to inform funding decisions for the 2019 Spending Review".[328]

87. External scrutiny of the 2022 NCS's implementation is nevertheless lacking, along with any information through which to conduct that scrutiny. The Progress Report does

[323] Referred to in the Strategy as the National Cyber Security Programme

[324] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022

[325] Red, amber or green

[326] Cabinet Office, National Cyber Strategy 2022 Annual Progress Report 2022–2023, 14 August 2023

[327] National Audit Office, Progress of the 2016–2021 National Cyber Security Programme (HC1988), 15 March 2019

[328] National Audit Office, Progress of the 2016–2021 National Cyber Security Programme (HC1988), 15 March 2019

not give any indication of the Government's current assessment of its performance against each outcome or sub-outcome but is rather a qualitative summary of the Government's achievements and future plans. There are very few updates in relation to some outcomes, including two that are crucial to the ransomware approach: that "Most serious state, criminal and other threats are routinely and comprehensively investigated", and that there will be an "increase in criminal justice and other disruptive outcomes for cyber criminals". We return to both topics in Chapter 6.

Oversight and ownership

88. Some witnesses suggested that responsibility within central Government for ransomware is unclear, with one arguing that "the large number of departments and bodies with overlapping functions and powers can hinder effective governance".[329] While the Home Office takes the lead on policy and oversees the NCA, many other parts of Whitehall also play significant roles in the ransomware response, including the Cabinet Office (which leads on cyber security policy), the Department for Science, Innovation and Technology (cyber skills), the FCDO (cyber diplomacy and GCHQ/NCSC) and the Ministry of Defence (the National Cyber Force). In addition, Lead Government Departments have responsibility for the cyber resilience of different CNI sectors, and under the National Risk Register they 'own' the management of risk related to major cyber-attacks within their remits.[330] Graeme Biggar conceded that ownership of cyber security is "inevitably diffuse".[331]

89. To coordinate this work, we were told that a Home Office-led Senior Ransomware Steering Group (SRSG) "brings together cross-HMG policy, intelligence and law enforcement partners", to oversee "all recommendations and updates that Ministers receive" across Government.[332] When we asked for its Terms of Reference, we were told that it meets monthly to discuss "live policy issues and operational activities including, but not limited to, international and industry engagement and our use of sanctions designations."[333] As a national security threat, ransomware also falls within the remit of the NSC, along with implementation of the National Cyber Strategy.[334] The NSC's broad remit and monthly cycle of meetings means, however, that ransomware is rarely likely to receive focused attention. There are currently four NSC sub-committees, covering Resilience, Europe, Economic Security and Nuclear, with none having specific responsibility for cyber matters.[335]

90. We have previously criticised the Government for its lack of Ministerial ownership on key national security threats, including cyber security.[336] In evidence to this inquiry, the Government was at pains to highlight that the Deputy Prime Minister (DPM) had

[329] FTI Consulting LLP, Clifford Chance LLP (RAN0034)

[330] HM Government, UK National Leadership for Risk Identification, Emergency Preparedness, Response and Recovery, August 2023

[331] Q55

[332] Cabinet Office (RAN0018)

[333] Cabinet Office (RAN0040)

[334] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022

[335] Under previous administrations, an NSC sub-committee on Cyber met for just over a year, between 2016 and 2017. Source: JCNSS, Cyber Security of the UK's Critical National Infrastructure: Third Report of Session 2017–19 (HC222/HL1708), 12 November 2018

[336] JCNSS, Cyber Security of the UK's Critical National Infrastructure: Third Report of Session 2017–19 (HC222/HL1708), 12 November 2018

clear responsibility for cyber security, including the implementation of the National Cyber Strategy and the cyber resilience of UK CNI. The DPM delivered a major cyber security speech in April, in which he stated that ransomware continues to "run rampant" and must be treated as a national security threat.[337] The DPM told us that "cyber has featured one way or another in pretty much every meeting" of the National Security Council resilience committee. The Home Office nevertheless claims the lead on ransomware as a policy issue, due to the Home Secretary's "specific responsibility to counter cyber crime".[338] When asked whether the DPM would consider setting up a ministerial committee on cyber, he said:

> I do not want committees that are established and then do not meet very frequently or do not provide a genuine forum by which we can collectively make decisions as a Government or hold departments to account. I am confident that the existing structure is sufficient … I am confident that the existing structure is sufficient.[339]

91. **The Government has acknowledged that ransomware is the number one cyber security threat to the UK. It is therefore welcome that it has published an ambitious National Cyber Strategy (NCS), with some strong commitments on resilience and the cyber security of core Government functions, both of which are vital to defending the UK against ransomware. It is also positive that the Cabinet Office has identified the Deputy Prime Minister as holding ministerial responsibility for the National Cyber Strategy, and that there is a cross-government steering group of senior officials to drive delivery work on ransomware. This is a better state of affairs than we have uncovered for some other cross-Government security risks. Nevertheless, there is still a lack of emphasis on prevention and a clear understanding of preventative measures. We remain concerned by the lack of cross-government ministerial fora for overseeing NCS implementation, given the National Security Council's very wide remit and limited schedule of meetings.** ***The Government should establish an NSC sub-committee on the National Cyber Strategy, which should consider progress against each of the five 'pillars' at least twice per year.***

92. **The National Audit Office (NAO) criticised previous delivery failures in cyber security in 2019, finding that the Government risked making the same mistakes with its subsequent National Cyber Strategy. The Government's Performance Framework for the 2022 NCS appears to be a reasonably rigorous approach to monitoring delivery, but its latest Progress Report sheds little light on whether it will achieve the NCS's ambitious objectives, particularly on disrupting and deterring offenders. Given the criticality of the NCS to the UK's national security and prosperity, it is vital that the Government's progress in implementing the NCS is exposed to external scrutiny.** ***We recommend that the NAO reviews the Government's progress in implementing the National Cyber Strategy through the National Cyber Programme and associated departmental activities, and the effectiveness of the NCS Performance Framework at monitoring and driving delivery.***

[337] For example: Cabinet Office, CyberUK speech, delivered on 18 April 2023

[338] Cabinet Office (RAN0018)

[339] Q81

The National Cyber Programme's merger with the CSSF

93. Funding for delivering the National Cyber Strategy is a mixture of departmental and programmatic spend, with £114 million identified in the Strategy for delivery of the National Cyber Programme[340] over the subsequent three years. Parts of the Government's overseas work on cyber have also been delivered through the Conflict, Stability and Security Fund (CSSF), which has increasingly focused on the cyber resilience of overseas partners.[341] Although the CSSF has experienced drastic cuts in recent years, driven largely by reductions in Official Development Assistance (ODA),[342] the scheme's cyber funding has increased five-fold since the portfolio was established in April 2020, from £5 million in 2020–21[343] to an allocation of £26 million for 2022–23.[344] Projects have included support for the development and implementation of Georgia's National Cyber Strategy, support for Ukraine, and investment in INTERPOL's cyber work.[345]

94. The 2023 Integrated Review Refresh effectively announced the abolition of the CSSF and the creation of a new fund, the Integrated Security Fund (ISF), which has the very wide scope of supporting the implementation of "key IR objectives, in the UK and overseas".[346] We were informed in May that the ISF will also incorporate the National Cyber Programme (NCP). At the Ministerial evidence session on 15 November the Deputy Prime Minister confirmed the ISF fund would not be 'ring fenced'[347] and has committed to update the committee on allocations of the fund once confirmed.[348] However, in our recent report on the CSSF, we expressed concerns that that the CSSF's objectives will be diluted by the ISF's much broader aims,[349] and the same could also be true of the NCP. It's also unclear why the Government has chosen to add a largely domestic funding pot to the CSSF, which has been spent almost entirely on overseas projects in the past.

95. **It is potentially concerning that the Conflict, Stability and Security Fund (CSSF) has now been merged with the National Cyber Programme—which delivers aspects of the National Cyber Strategy—as part of the new Integrated Security Fund (ISF). We recognise that this could encourage a more integrated approach to the UK's domestic and international cyber work, enhancing our allies' resilience against ransomware actors and addressing threats to the UK's critical supply chains. Given the wide remit of the ISF, however, there is also a risk that cyber work could be deprioritised against other security objectives, at a vital time for the UK's active engagement on cyber security with our international partners. Funding for overseas work also risks being diverted towards domestic priorities, in the face of political pressures closer to home—a risk that we also highlighted in our recent report on the CSSF.**

[340] Programmatic spend

[341] HM Government, Conflict, Stability and Security Fund: Annual Report 2021/22, 26 January 2023

[342] HM Government, Integrated Review Refresh 2023: Responding to a more contested and volatile world (CP 811), March 2023

[343] HM Government, Conflict, Stability and Security Fund: Annual Report 2021/22, 26 January 2023

[344] HC Statement HCWS525, 26 January 2023

[345] CSSF Programme Summary: Cyber & Tech Security Programme, 2020/21 - 2022/23

[346] HM Government, Integrated Review Refresh 2023: Responding to a more contested and volatile world (CP 811), March 2023

[347] Q82

[348] UK Government (RAN0042)

[349] JCNSS, The Conflict, Stability and Security Fund: Second Report of Session 2022–23 (HC1389/HL253), 20 September 2023

96. ***To ensure ongoing transparency and accountability, the Government's Annual Progress Report on the National Cyber Strategy should remain distinct from any Annual Report on the Integrated Security Fund, and should specify how the Government is using ISF funding to deliver NCS objectives. Through its Annual Report and statements to Parliament on the ISF, the Government should continue to make clear the regional, programmatic and thematic allocations for the Fund, as it has done for the CSSF. Finally, as recommended in our recent report on the CSSF, the Government should similarly maintain the CSSF's current levels of transparency in the publication of information on programme activity, spend and performance.***

Leadership and political will

97. The Government's written evidence stated that ransomware was a "top priority", and the NCA told us that it has regular engagement with the Home Secretary on cyber security, reassuring us that her "interest is very real".[350] Beyond the operational level, however, some witnesses questioned whether this was the case: RUSI argued that the Home Office's 2022 ransomware 'sprint'[351] led to "no discernible shift in the government's overall approach", and concluded that the NCSC's efforts have not been matched by ministerial interest. It called instead for a more "strategic approach", to "reflect the fact that ransomware–and organised cybercrime more generally–is a persistent and potentially acute threat to UK interests". Starkly, it suggested that Government's response might be improved by moving responsibility for ransomware policy development from the Home Office to the Cabinet Office, or even to the NCSC, to increase ministerial interest and political will.[352] At the very least, it argued, the Home Office should "upskill policy leads to provide a more rigorous understanding of the nature of the threat".[353]

98. RUSI's frustration may reflect the fact that it called for "urgent policy intervention" on ransomware in 2021;[354] since then, very little has changed in the policy landscape, despite ongoing operational efforts by the NCSC and NCA—and in contrast to online fraud, which is benefiting from a new national strategy and additional resources. RUSI's evidence also echoes the findings of an exposé in *The Record* (a cyber news outlet) in 2022, informed by anonymous civil servants, in which it was reported that the level of ministerial interest in ransomware was not proportionate to the scale of the threat, with small boat crossings in the English Channel prioritised by successive Home Secretaries. Again, it noted that the ransomware sprint delivered no tangible outcomes and was focused instead on increasing awareness of the scale and complexity of the threat, reflecting "more about the government's starting position than where it finished". Officials reportedly told *The Record* that they "saw no light at the end of the tunnel" for ransomware.[355]

[350] Q55

[351] According to the Government's written evidence, HMG "launched a cross-Government ransomware "sprint" that ran from June 2021 to February 2022. The sprint[2] involved a number of Whitehall Departments[3], operational partners[4] and law enforcement[5]. It explored existing ransomware policies, areas of potential improvement, and culminated with a series of recommendations to Ministers. Since then, the Home Office has continued to lead cross-Government ransomware work under the Threat Pillar of the National Cyber Strategy."

[352] Royal United Services Institute (RAN0032)

[353] Royal United Services Institute (RAN0032)

[354] RUSI emerging insights (James Sullivan and James Muir, Ransomware: A Perfect Storm, March 2021

[355] The Record, Ransomware incidents now make up majority of British government's crisis management COBRA meetings, 18 November 2022

99. We recognise that public output is just one measure of political interest, but it can be a strong indicator of the extent to which Ministers are consumed by a topic. In light of the anonymous comments made to *The Record*, we compared public statements on ransomware with those on another major policy issue—small boats. We found that the Home Office's public output on cyber security and ransomware has been almost non-existent, and has been dwarfed by its focus on small boats and illegal migration.[356] The Security Minister recently provided the foreword to an NCSC report on "Ransomware, extortion and the cyber crime ecosystem", which set out the current nature of the threat; despite being described as a 'white paper', however, it contained no proposals for policy or legislative reforms.[357,358]

100. The Government's legislative programme also suggests that cybercrime has not been a significant priority for Home Office Ministers, beyond the new offences on online content and data created by the Online Safety Act 2023[359] and the National Security Act 2023.[360] Following a consultation on modernising the Computer Misuse Act 1990 (CMA) in 2021, the Government then delayed taking any further public action until earlier this year, when it launched a second consultation. The day prior to the Ministerial session the Home Office published their analysis of the consultation but made no concrete commitment to legislating soon. At the Ministerial session on 15 November, the Minister for Security acknowledged how out of date the CMA was.[361] We return to the need for CMA reform in further detail in the next chapter.

101. **The Home Office claims the lead on ransomware as a national security risk and policy issue, but the then Home Secretary, Suella Braverman MP, showed no interest in it. According to some observers, clear political priority is given instead to other issues, such as illegal migration and small boats. We recognise the significance of illegal migration as a policy challenge, but there is a risk that ransomware is relentlessly deprioritised. The Department's ransomware 'sprint' in 2022 resulted in no discernible policy outcomes. The Minister for Security's acknowledgement of how out of date the Computer Misuse Act is does not excuse the lack of progress which has been made to legislate in this space. It has been two-and-a-half years after its main consultation and 33 years since that dated legislation received Royal Assent. It is hard to see how the Criminal Justice Bill brought forward by the King's Speech 2023 will sufficiently cover the gap left by the outdated CMA.**

102. ***In line with many other aspects of cyber security, and to ensure that it is treated as a cross-government national security priority, responsibility for tackling ransomware***

[356] The former Home Secretary The Rt Hon Suella Braverman KC MP made 63 spoken contributions in the Commons Chamber referencing small boats since her appointment a year ago, compared with one on ransomware (mentioned in passing in relation to the Economic Crime and Corporate Transparency Bill), and no contributions on cyber security more broadly. The Security Minister has also referenced ransomware once. The former Home Secretary made five Ministerial Statements on small boats (as well as her speeches on the Illegal Migration Bill), but none on ransomware. Since his appointment to Home Secretary on 13 November, James Cleverly has issued 2 written statements on illegal migration and mentioned illegal migration 23 times. He has not mentioned ransomware.

[357] NCSC and NCA, Ransomware, extortion and the cyber crime ecosystem: A white paper from the NCSC and the NCA, September 2023

[358] According to Cabinet Office guidance, a White Paper includes "major policy proposals set out in more detail" (than a green paper discussion or consultation document). Source: Cabinet Office, Guide to Making Legislation, August 2022

[359] Online Safety Act 2023

[360] National Security Act 2023

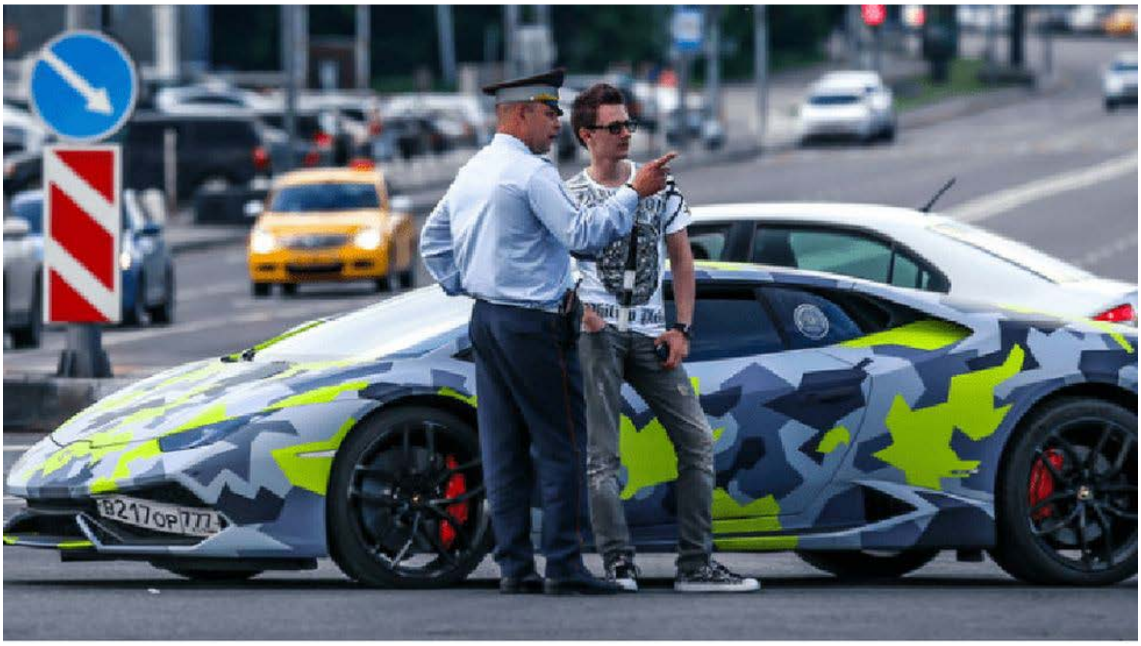
[361] Q84

should be transferred from the Home Office to the Cabinet Office, in partnership with the NCSC and NCA. It should also be overseen directly by the Deputy Prime Minister, as part of a holistic approach to cyber security and resilience.

6 Raising the costs for attackers—who pays?

103. A young man stands nonchalantly next to a camouflage-printed car, in discussion with a uniformed Russian police officer. The car is easily identifiable as a custom Lamborghini Huracan, retailing for around £150,000; the numberplate reportedly reads "THIEF" in Russian.[362] The individual is the 36-year old, Ukrainian-born Maksim Yakubets, believed to be a 'ringleader' in the Russian-based Evil Corp group, behind a string of attacks against financial institutions and once identified by the NCA as "the most significant cybercrime threat to the UK".[363] The US has sanctioned and indicted Yakubets, but he reportedly remains at large in Russia.[364] He married the daughter of a former FSB officer in 2017, in a "lavish" ceremony at a golf club near Moscow.[365]

Figure 2: Maksim Yakubets, believed 'ringleader' in the Russian-based Evil Corp group in discussion with a Russian police officer



104. This striking image of Yakubets illustrates two glaring realities: first, the vast profits to be gained from ransomware and other linked cybercrimes; and second, the immense challenges involved in bringing perpetrators to justice, in the context of Russia's tacit approval of ransomware operations against the West. This chapter considers broader law enforcement efforts to tackle ransomware offending, and whether law enforcement agencies are adequately resourced to disrupt and deter ransomware gangs.

Law enforcement capabilities and resources

105. The Russian origin of most ransomware attacks is clearly a major obstacle to 'traditional' law enforcement outcomes, and the Government told us that "criminal justice

[362] *The Times*, Moscow 'cyberthief' wanted for stealing millions from Britons, 6 December 2019

[363] *The Times*, Moscow 'cyberthief' wanted for stealing millions from Britons, 6 December 2019

[364] *BBC News*, Evil Corp: 'My hunt for the world's most wanted hackers', 17 November 2021

[365] *The Sun*, CRIME PAYS: Inside lavish £250k wedding of Russian super hacker branded the world's worst cybercriminal by Britain and US, 12 December 2019

outcomes against High End of High Harm (HEHH) [ransomware] offenders are often unrealistic”.[366] Nevertheless, the FBI has achieved some notable disruptions of ransomware operatives, including its recent penetration of the Hive group, reportedly saving $130 million in potential ransom payments.[367] Witnesses praised the US Government’s approach for going beyond “the traditional ‘investigate, arrest, name and shame’ approach” and towards a strategy of “long-term infiltration of these groups by intelligence and law enforcement”, which includes “disrupting their infrastructure, stealing decryption keys from them or even just sowing distrust and paranoia within these communities”.[368]

106. The UK’s National Cyber Strategy commits to ensuring that, by 2025, malicious cyber actors are “less able to target the UK as a result of our disruption and denigration of their activities and capabilities”.[369] The Government’s written evidence made only brief references to the need to disrupt ransomware operators, however, noting that the NCCU has been “required to develop a range of alternative disruption methods” as part of its ransomware response, and that the NCA “uses a variety of tactics and niche capabilities to identify and disrupt offenders”. This includes “monitoring their travel, dismantling wider criminal networks (including those developing and deploying ransomware), tackling criminal infrastructure and marketplaces, and targeting their financial flows”. In contrast, it dedicated 20 paragraphs to resilience, and asserted that this is “the key to combating ransomware”.[370] The Government’s recent Annual Progress Report on the National Cyber Strategy also had little to say on this topic, beyond the use of sanctions and the expansion of the National Cyber Force.[371]

107. Witnesses have criticised the Government for its primary focus on resilience,[372] and even Graeme Biggar referred to “long debates about the balance within [the National Cyber Strategy] between, for example, resilience and disrupt”.[373] RUSI has called for a more aggressive approach:

> The UK’s strategic approach should reflect the fact that ransomware—and organised cybercrime more generally—is a persistent and potentially acute threat to UK interests. **The government cannot simply build a big wall around the UK through resilience-building measures alone**, it must be more aggressive and persistent in pursuing and disrupting the cybercriminal ecosystem and economic model. This is an issue of mentality as much as it is policy and resourcing.[374] [Emphasis added]

108. The NCA has some offensive capabilities, as we saw when we visited their offices in February. It has also supported cross-border operations with the FBI and other partners, including the Hive ‘hack-back’ referenced earlier.[375] We questioned Graeme Biggar about

[366] Cabinet Office (RAN0018)

[367] *Computer Weekly*, Hive ransomware gang taken down after FBI hacks back, 27 January 2023

[368] Q42 (Jamie MacColl)

[369] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022

[370] Cabinet Office (RAN0018)

[371] Cabinet Office, National Cyber Strategy 2022 Annual Progress Report 2022–2023, 14 August 2023

[372] For example: PlatinumHIT (RAN0026)

[373] Q54

[374] Royal United Services Institute (RAN0032)

[375] NCA News, HIVE takedown: NCA in international operation to shut down $100m ransomware threat, 26 January 2023

these joint operations, however, and he acknowledged that the US has been "much more successful than us" at disrupting ransomware operatives. He attributed this to two main factors—legislation and resourcing:

> [The US] has invested in it more than we have as a country and we have as the NCA—mea culpa. Also, its legal framework makes it easier for it to do that. […] We have been involved with the FBI on some major investigations and take-downs, and on too many of them it has been the FBI in the lead and us supporting. We would like to be in a position where the FBI comes in to support us.[376]

109. Having experienced joint US-UK working while at the FBI and the US Department of Justice, John P. Carlin called for the NCA to receive more funding, so that it could "sufficiently and adequately meet its mandate, both within the United Kingdom and in cooperation with its foreign partners".[377] Graeme Biggar was also clear that resources remain a major issue for the NCA, which he described as "the classic challenge for serious organised crime". He told us that the agency has failed to meet the growing demands from the exponential growth in cybercrime, and that a more significant shift is required:

> […] I do not want us to give the impression that this is fine, it is completely resourced and we have got it. If you take a step back from ransomware and look at crime affecting the UK, one of the major trends […] is more crime going online and more of the crime that is not online being supported by technology. That is a really significant shift […] that has not yet been accompanied by a similar shift from law enforcement, including the NCA, and ransomware is then one part of that.[378]

Mr Biggar noted that the Government has funded Regional Cyber Crime Units as well as the NCA, as touched upon in Chapter 4, but commented that this is still a "relatively small" resource, adding: "we are talking 250 people in the National Crime Agency and 300 spread around the regions".[379]

110. We subsequently examined NCA resources in further detail, and found that the 250 individuals working in the NCCU represent only 5% of the NCA's 5000-strong workforce, and that the NCCU is less than a sixth the size of the FBI's cyber division.[380] The NCA has also struggled to recruit as a result of increasing pay differentials with policing: in its submission to the NCA Remuneration Review Body last year, it pressed for "a pay and benefits framework that will enable us to attract and retain the capabilities that we require".[381] The Review Body concluded that the NCA's pay ambitions were "unaffordable" (within the narrow remit it was given by the Government). It also noted that "It is for the NCA to negotiate its funding with the Home Office and HM Treasury, but both those organisations also have a responsibility for ensuring the Agency has the resources it needs to lead the fight against serious and organised crime".[382] The Minister for Security told us

[376] Q58

[377] John P. Carlin (Partner, Cybersecurity & Data Protection practice at Paul, Weiss, Rifkind, Wharton & Garrison LLP) (RAN0038)

[378] Q54

[379] Q57

[380] National Crime Agency (RAN0039)

[381] Home Office, NCA and NCA Remuneration Review Body, Evidence to the NCA Remuneration Review Body (NCARRB), 2022 to 2023, 10 August 2022

[382] National Crime Agency Remuneration Review Body, Eighth Report 2022 (CP790), February 2023

that "the NCA salary comparators are very difficult to make, because the NCA employs on different bases depending on whether people are employed through the UK Intelligence Community as warranted officers or are part of the Civil Service."[383] But he acknowledged that it was " very difficult to compete with the private sector for the kind of skills and salary levels that we are able to command in government."

111. The NCA's recruitment challenges sit against a backdrop of significant long-term cyber skills shortages in the UK: the Government notes that there was "a shortfall of c.14,100 people in the UK cyber security workforce in 2021",[384] but one witness put the gap at 57,000, reflecting a 73% increase in unmet demand since 2021.[385] Addressing the cyber skills shortage is a prominent focus of the National Cyber Strategy, which pledges to achieve a "significant increase in the number of people who have the skills they need to enter the cyber workforce" by 2025,[386] but the latest Annual Progress Report acknowledged that there "remains more to do to ensure that the UK economy is producing the skills that it needs".[387] Even in this challenging context, Mr Biggar noted that the NCA's pay challenges put the organisation at "more of a disadvantage" than the police and other parts of the public sector when seeking specialist cyber skills.[388]

112. **The National Crime Agency is locked in an uphill struggle against the ransomware threat, which is now so sophisticated that even the most highly-protected organisations expect to experience a ransomware attack. There is clear value in the Government's resilience work, but it is vital that this is paired with further work to raise the costs for attackers, to make the UK a less attractive target. Based on the evidence we have seen, the NCA has insufficient resources and capabilities to match the scale of this challenge.**

113. **It is possible to infiltrate and disrupt ransomware groups' infrastructure without arresting the criminals involved, sometimes even preventing attacks after the initial infiltration has taken place. The NCA has some offensive capabilities, but it is vital that the UK is able to operate on a level footing with its international partners.** ***The Government should invest significantly more resources in the NCA's response to ransomware, enabling it to pursue a more aggressive approach to infiltrating and disrupting ransomware operators.***

114. **The NCA's resourcing challenges are exacerbated by the Government's failure to allow them to offer salaries that might attract those with specialist skills. It will always be difficult for the NCA to compete with the private sector, particularly for roles requiring high-level cyber skills, but it is unacceptable that NCA officers are paid less than their policing counterparts. As the elite national squad for serious and organised crime, the public would rightly expect the NCA to offer a competitive pay package, in recognition of the more specialist skills required for defending the UK against serious organised crime.** ***The Home Office and Treasury should urgently revisit the funding available for NCA pay and progression, which has been an obstacle to achieving pay parity between police forces and NCA officers.***

[383] Q85
[384] Cabinet Office (RAN0018)
[385] (ISC)^2 (RAN0010)
[386] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022
[387] Cabinet Office, National Cyber Strategy 2022 Annual Progress Report 2022–2023, 14 August 2023
[388] Q59

The role of the UK intelligence community

115. The NCA is not the only Government agency involved in pursuing cyber threat actors.[389] Their efforts to tackle the criminal aspects of the ransomware threat are supplemented by those of the National Cyber Force (NCF), which has "increased its operational output" over the last year.[390] The NCF operates "in and through cyberspace to keep the country safe and to protect and promote the UK's interests",[391] including through operations against both state and non-state threat actors.[392] This encompasses work by GCHQ and the Secret Intelligence Service.

116. Political decisions about resourcing and agency responsibilities are tightly linked to the Government's understanding of the nature of any threat. The Government's Integrated Review Refresh recognised that the barriers between the threat categories handled by these agencies—serious organised crime for the NCA and hostile state threats for the intelligence agencies—are increasingly porous, however, and that "the capabilities and activities we use to respond to and disrupt them are increasingly overlapping".[393]

117. Ransomware appears to be a stark illustration of the sort of blurred lines depicted in the IRR. As we concluded in Chapter 2, the Kremlin's involvement in most ransomware attacks is often likely to be indirect, through the tacit endorsement of ransomware operatives and their ability to conduct attacks against Western targets without fear of domestic reprisal. The NCSC—a wing of GCHQ—is nevertheless involved in ransomware incident response work for the most serious cases. Witnesses told us that ransomware is both a national security threat and a criminality issue, and that it needed to be regarded as both:[394] the NCC Group called on the UK to draw from the US's 'full statecraft' approach to ransomware,[395] and John P. Carlin noted that a "blended threat" requires a blended approach.[396] He warned against taking a more siloed approach, drawing on lessons learned from the 9/11 terror attacks:

> In the United States, we have taken what we call an "all-tools" approach, which is based on the lessons that we learned post September 11 but frankly were not applying to the cyber realm until about 10 years ago […]. […] One of the failures of September 11 was the failure to adequately share information within government and across law enforcement, from the criminal to the national security community […].
>
> When I moved from being chief of staff at the FBI to running the national security vision at [the Department of] Justice, I saw similarly, when it came to cyber, that we treated certain offences, such as cyberattacks, as criminal, and then looked at national security actors, nation state actors, as

[389] Unlike in the US, where the FBI's responsibilities encompass both criminal and national security (including foreign intelligence threats), the NCA is tasked purely with tackling the criminal aspects of the ransomware threat. Source: National Crime Agency (RAN0039)

[390] Cabinet Office, National Cyber Strategy 2022 Annual Progress Report 2022–2023, 14 August 2023

[391] HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, 15 December 2022

[392] National Cyber Force, The National Cyber Force: Responsible Cyber Power in Practice, April 2023

[393] HM Government, Integrated Review Refresh 2023: Responding to a more contested and volatile world (CP 811), March 2023

[394] For example: Q35

[395] NCC Group (RAN0012)

[396] Q35 (John P. Carlin)

> an intelligence problem. But we were not putting the information together to see whether we could use every available legal tool, some of which came from criminal authorities and some from national security.[397]

118. RUSI made a rather damning assessment of UK agencies' current ability to apply such a full-spectrum response to the ransomware threat, however. Its evidence argued that "it is not clear that the UK's national security apparatus and intelligence community is sufficiently motivated and resourced to prioritise ransomware or other forms of organised cybercrime alongside nation-state cyber threats". It added:

> Although Lindy Cameron, the CEO of the NCSC, has been vocal in highlighting the threat posed by ransomware to national security, these efforts have not been matched by ministerial interest in the Home Office, Cabinet Office or DCMS. This has implications for the allocation of time, resources and technical expertise that can be directed towards the ransomware threat.[398]

Jamie MacColl reiterated this message when he gave evidence to us in April, arguing that the UK intelligence community does not regard ransomware "to be a threat on the same level as state threats or terrorism", and that the national security 'apparatus' is "not that comfortable dealing with cybercrime".[399]

119. **The Government and NCSC's approach to ransomware is often framed through the language of state threats. While we recognise that operators are often facilitated by the Russian harbour state, ransomware is primarily a problem of criminality for profit, rather than espionage or geopolitical sabotage. Through the 2021 Integrated Review and its 2023 Refresh, the Government has acknowledged that the blurred lines between state threats and serious and organised crime require more threat-agnostic capabilities—and yet ransomware is currently at risk of falling into a 'no man's land' between state threats and criminality.**

120. **Given the links between ransomware crime and certain state actors, it is striking how little attention has been paid to the potential for international law to target the collusion of states. In Chapter 2, our report highlights the possibility that Russia's approach could constitute a violation of international law.** ***Recognising that Russia shows little, if any, respect for international law, the FCDO should nevertheless investigate the possibilities for legal sanctions and international cooperation to deter state-linked ransomware crime.***

121. **The Government's response to ransomware is conducted partly through the National Cyber Force and the intelligence agencies, on which we can only access limited information. RUSI has argued that the UK intelligence community may not be sufficiently motivated or resourced to tackle ransomware, but it is vital that the NCA's work is properly supplemented by the other agencies.** ***In light of these concerns, and to ensure full scrutiny of state capabilities on ransomware, we recommend that the Intelligence and Security Committee scrutinises the extent and nature of the resources and capabilities devoted to disrupting ransomware operatives by the intelligence agencies, as opposed to combating broader state-sponsored cyber threats. We also recommend***

[397] Q35
[398] Royal United Services Institute (RAN0032)
[399] Q39

that the Committee examines how the intelligence agencies work in partnership with the NCA to deploy a full-spectrum response to the ransomware threat, as envisaged by the Integrated Review and IR Refresh, and how this compares with the US agencies' 'full statecraft' approach to ransomware.

Crypto-assets

122. The exponential growth in ransomware has been attributed, in part, to the ease with which attackers can obtain payment in virtual currencies.[400] Cryptocurrencies or 'crypto-assets' are a digital means of financial exchange,[401] and are the main payment method demanded by ransomware operatives. The resulting funds might then be laundered through financial networks until they can be used standard currency, or they may be used to fund further ransomware attacks (through ransomware-as-a-service models). Ransomware remains a lucrative activity as a result: a UK cyber security firm claimed recently that the average UK ransom payment in 2023 was $2.1 million.[402] Chainalysis, a US 'blockchain' analysis company,[403] identified total global ransomware payments of US$712 million in 2021, which it described as an "underestimate".[404]

123. The Economic Crime and Corporate Transparency Act 2023 will give law enforcement agencies new powers to seize crypto-assets,[405] Aidan Larkin, a crypto expert and CEO of Asset Reality,[406] described the Act's reforms as "superb", adding that they will "make it much easier for law enforcement to do what it needs to do". He nevertheless warned that law enforcement agencies are technically already able to 'follow the money' in a crypto transaction, but "there are not enough people, tools or training to do that work."[407] Regardless of the legislation, he likened the lack of capabilities and resources to "having an international airport without yet having X-ray equipment, sniffer dogs or financial intelligence capability".[408] As a result, the UK's civil recovery and criminal asset recovery statistics "make for horrific reading".[409]

124. This may be another area in which the UK is falling behind the US. After the Colonial Pipeline attack in June 2021, the US Department of Justice successfully seized the majority of the US$4.4 million ransom paid by the victims.[410] Aidan Larkin said that IRS[411] criminal investigations have resulted in crypto seizures of over $10 billion (not all linked to ransomware), and that the Home Office is falling short in comparison:

[400] Crowd Strike, History of Ransomware, 10 October 2022; FTI Consulting and Clifford Chance WE

[401] House of Commons Library, Cryptocurrencies (Research Briefing 8780), 22 February 2023

[402] *The Guardian*, Ransomware payments nearly double in one year, 10 May 2023

[403] According to Chainalysis: "With blockchain analysis, using one ransomware-related digital asset address, a trained investigator can identify not only which address currently holds the fund but which other addresses are associated with that ransomware actor, as well as which facilitating tools and services enable their attacks, such as access brokers, VPN providers or bulletproof hosting services, and which other groups these actors may be collaborating with." Source: Chainalysis Inc. (RAN0008)

[404] Chainalysis Inc. (RAN0008)

[405] The Economic Crime and Corporate Transparency Act 2023

[406] Asset Reality is a company that offers a " seized asset management platform" to law enforcement agencies, lawyers, investigators and insolvency practitioners.

[407] Q52

[408] Q50 (Aidan Larkin)

[409] Q42

[410] *Thomson Reuters*, Recovery of Colonial Pipeline ransom funds highlights traceability of cryptocurrency, experts say, 23 June 2021

[411] Internal Revenue Service - the US Government's tax collection authority

> What worries me is that the levels of adoption and of crypto activity that we have in the UK are not seen in the Home Office statistics for crypto asset recovery returns. Where are the billion-dollar seizures, the £100 million seizures or even the £10 million seizures? The Metropolitan Police, the NCA and others have reported some excellent statistics on crypto seizures, but not at the rate that you would expect for the amount of crypto activity that is going on here.[412]

The NCA reported seizing nearly £27 million in cryptocurrencies in 2021/22, dropping to £16.4 million in 2022/23 (a fall of 39%); it is unclear how much of that relates to ransomware.[413] Graeme Biggar told us that the agency is currently "building up a new team on cryptocurrency", recognising the importance of enhancing its expertise;[414] the Home Office is also examining "technological capabilities across the system" for pursuing crypto payments.[415]

125. **Crypto-assets are the lifeblood of the ransomware ecosystem, and have been a major driver of the increased threat. The Government is making welcome reforms to the UK's legislative regime underpinning crypto-asset seizure, but we have heard that the NCA has insufficient capacity and skills to make full use of its existing powers, which might be why its total crypto seizures decreased by over a third between 2021/22 and 2022/23. It is essential that the UK bears down on the vast profits of these criminal groups.** ***The Government and NCA must prioritise further resources towards the training and recruitment of officers with skills in crypto-asset trace and seizure, to reduce the incentives for criminals and to claw back some of the financial losses experienced by ransomware victims.***

Legislation

126. The pace of legislative reform on crypto-assets has not been matched by cybercrime more broadly. Although the Online Safety Act 2023 creates new online offences, it fails to address deficiencies in the main legislative framework for cybercrime—the Computer Misuse Act (CMA) 1990, which criminalises unauthorised access to computer systems and data.[416] Rob Jones noted that the legislation "did not envisage the digital age we now live in or the exponential growth in threat as well as the success of the internet". The CMA was intended to target "people stealing each other's passwords and doing stupid things on computers", and not "elite Russian-speaking actors targeting the UK and extorting millions of pounds".[417]

127. As we touched upon in Chapter 5, the Home Office has acknowledged that reform is required: in its initial consultation on the CMA, held from May to June 2021, it noted that "the Act was passed 30 years ago, and since then the reliance of society on the digital world has increased enormously".[418] Two and a half years on, however, the legislation remains out of date: the Department has instead consulted again on reform, outlining what it

[412] Q51
[413] National Crime Agency, Annual Report and Accounts 2022 - 2023 (HC1479), 18 July 2023
[414] Q59 (Graeme Biggar)
[415] Cabinet Office (RAN0040)
[416] Home Office, Review of the Computer Misuse Act 1990: consultation and response to call for information, 20 February 2023
[417] Q56
[418] Home Office, Computer Misuse Act 1990: call for information, 11 May 2021

proposes to change and asking for further views. On 14 November 2023, the Government published the Review of the Computer Misuse Act 1990.[419] The publication pointed to three areas for further consideration; domain and IP address takedown and seizure, power to preserve data, and data copying. However, on all three the Government indicated they would either engage further with stakeholders or "provide further legislative solutions in the near future".[420] Given the links to state threats, the reforms could arguably have been introduced as part of the (wide-ranging) National Security Act, which received Royal Assent in July.

128. There can be little doubt that these delays are causing operational problems. The NCA told us that the lack of extra-territorial provisions for CMA offences is an "impediment" to the law enforcement response, and that reforms to enable them to seize domain names and IP addresses would "prove vital in enabling NCA to pursue criminals and disrupt the cybercrime ecosystem".[421] It is calling for the Government to introduce a number of reforms[422]—all of which we recommend below—and all of which were either proposed or further consulted upon in the latest Home Office consultation.[423]

129. **The UK's main legislative framework on cybercrime is over 30 years old. In that time, the country's relationship with the online world has changed beyond recognition, along with the scale and nature of cybercrime. Rather than introducing a Bill, however, the Home Office has run a second consultation on its proposed reforms to the Computer Misuse Act 1990 (CMA), and only published an analysis on 14 November 2023. We are disappointed that the King's Speech 2023 did not include the CMA and we are still unclear as to how the Criminal Justice Bill is a suitable replacement.** ***The Government should urgently bring forward legislation to reform the Computer Misuse Act, including to:***

- ***Criminalise the theft and copying of data, to bring it in line with property theft offences;***
- ***Introduce appropriate extra-territorial provisions for cybercrime;***
- ***Give authorities the power to preserve data, pending a decision on formal seizure;***
- ***Enable law enforcement agencies to seize domain name and IP addresses; and***
- ***Increase the maximum sentences for more serious CMA offences.***

130. **There is a high risk that the Government will face a catastrophic ransomware attack at any moment, and that its planning will be found lacking. In 2020, this Committee examined the Government's preparations for the Covid-19 pandemic, considering what it could teach us about how to prepare for a known risk with a high potential impact. We found that the Government had not prepared adequately for a pandemic, despite knowing that there was an increasing chance of such a scenario occurring. The**

[419] Home Office, Review of the Computer Misuse Act - Analysis of Consultation responses, 14 November 2023

[420] Home Office, Review of the Computer Misuse Act - Analysis of Consultation responses, 14 November 2023

[421] National Crime Agency (RAN0039)

[422] Q56 and National Crime Agency (RAN0039)

[423] Home Office, Review of the Computer Misuse Act 1990: consultation and response to call for information, 20 February 2023. Further consultation was considered necessary on the extra-territorial provisions and sentencing changes.

Government is at risk of making the same mistake again: it knows that the possibility of a major ransomware attack is high, yet it is failing to invest sufficiently to prevent catastrophic costs later on. There will be no excuse for this approach when a major crisis occurs, and it will rightly be seen as a strategic failure. If the UK is to avoid being held hostage to fortune and avoid electoral interference it is vital that ransomware becomes a more pressing political priority, and that further substantial resource be devoted to tackling this pernicious threat to the UK's national security.

Conclusions and recommendations

The scale and nature of the ransomware threat

1. A major ransomware attack could have a devastating impact on UK citizens and the economy, and undoubtedly represents a major threat to UK national security. A sophisticated ransomware ecosystem has evolved, with criminals able to purchase advanced forms of malware and access points in order to conduct profitable and damaging attacks. This has made it much more widely available to those who wish to inflict harm for profit, and increased the scale of the threat. (Paragraph 21)

2. Past attacks demonstrate that ransomware can cause severe disruption to the delivery of core Government services, including healthcare and child protection, as well as causing ongoing economic losses. Mass data loss from an attack can be irreversible, even when the ransom is paid. Given the damage wrought by these uncoordinated ransomware attacks, a coordinated and targeted attack has the potential to take down large parts of the UK's critical national infrastructure and public services and—in the words of the National Crime Agency—to bring the country to a standstill. It would also shine a spotlight on the inadequacy of the Government's efforts to secure the UK against ransomware, and to prepare for the aftermath of a major cyber-attack. (Paragraph 22)

3. Russian-speaking actors are the source of most attributable ransomware attacks against UK targets. The Russian Government's tacit (or even explicit) approval of these attacks is consistent with the Kremlin's disruptive, zero-sum-game approach to the West. It also provides revenue to the Putin regime's well-oiled network of corruption and criminality. This is not a straightforward state threat, however. For many Russian hackers, ransomware is simply an easy way to make large sums of money, with next-to-no chance of being caught or prosecuted. Regardless of the extent of state involvement, or whether they are ideologically driven rather than financially, the sheer scale of the threat demonstrates how vital it is that the UK is adequately resourced to upscale its defences, and to prepare for a major attack. (Paragraph 32)

Strengthening our defences — UK preparedness and resilience

4. The Government and the National Cyber Security Centre (NCSC)—the public-facing arm of GCHQ—have focused significant efforts on enhancing the UK's cyber resilience, with particular attention paid to major operators of critical national infrastructure (CNI). Nevertheless, UK CNI remains vulnerable to a catastrophic ransomware attack, particularly in sectors in which investment in upgrading legacy infrastructure has been inadequate. Supply chains are also particularly vulnerable, and have been described by the NCA as the 'soft underbelly' of CNI. With different CNI operators sharing the same supplier, a single attack could also affect multiple sectors at once, with damaging and widespread consequences. (Paragraph 43)

5. Unlike many areas of national resilience, the Government has imposed cyber resilience requirements on most CNI operators through the 2018 Network and Information System (NIS) regulations, and has also committed to imposing new

cyber resilience standards on CNI by 2025. There are significant issues with the implementation and oversight of the existing regulations, however, linked to a lack of regulator capability and cyber skills. Plans to extend the NIS regulations to CNI supply chains need to be accompanied by further work to ensure that they can be implemented effectively. *The Government must scope the feasibility of establishing a cross-sector regulator on CNI cyber resilience to oversee the implementation of the NIS regulations, and to make recommendations for investment and legislative reform. The Government should report back to us on the outcome of this scoping work by March 2024.* (Paragraph 49)

6. We welcome the Government's efforts to reinvigorate the National Exercise Programme. The majority of UK CNI is run by private operators, however, so it is vital that these companies are invited to participate in the Programme. The exercises should also consider broader impacts, beyond a single infrastructure sector. *As part of the National Exercise Programme, the Government should hold regular national exercises to prepare for the impact of a major national ransomware attack affecting multiple CNI sectors, engaging CNI operators to stress-test their response and ensure a swift recovery. It should also ensure that the insights from these exercises are fed back to Lead Government Departments and regulators, so that they enhance preparations for future potential attacks.* (Paragraph 53)

7. Although we recognise the value of peer support, it should not have fallen to Redcar and Cleveland Council's Leader to train other councils how to prevent and respond to cyber-attacks, following their own devastating attack in 2020. Local authorities are on the frontline of support for the most vulnerable in society. The Government needs to provide much more active support. This should include how to prevent and respond to major cyber-attacks, recognising the extremely challenging financial circumstances in which they operate. The Government's understanding and expectations regarding local aut.hority preparedness has developed since 2021. However the problem persists, the NCSC Annual Review for 2023 reported that 73% of reports to the NCSC Vulnerability Reporting Service have come from Local Government and local services. We recognise and welcome the work undertaken by the NCSC so far, but urge the Government to pursue a more focused effort which proactively seeks to support local government with preventative support and strengthened resilience measures. *The NCSC should be funded to establish an enhanced and dedicated local authority cyber resilience programme, including intensive support for local exercising and on securing council supply chains.* (Paragraph 58)

Responding to attacks — victim support and recovery

8. Many ransomware victims feel there is insufficient support from law enforcement or Government agencies, with limited state resources focused on the most critical organisations. For smaller organisations and those falling outside the boundaries of critical national infrastructure, the NCSC's post-incident support appears limited to a list of approved cyber incident response companies, which may be beyond the financial reach of many victims. These gaps in support apply to important elements of the public sector too, including schools and colleges, and stand in stark contrast to victim support for comparable thefts or ransom demands in the offline world. *The NCSC and NCA should be funded to provide negotiation, recovery and remediation*

capabilities to all public sector victims of ransomware, to the point of full recovery. The NCSC should also explore, with the cyber incident response industry, the possibility of establishing a 'pro bono', industry-led scheme for charities and small businesses, akin to those provided by many major law firms. (Paragraph 65)

9. The emphasis on supporting high-risk individuals and protecting electoral integrity is undoubtedly welcomed. We would, however, welcome a more direct approach from the NCSC in their offer of support to political parties and high-risk individuals. It is unclear if the support for 'high risk individuals' will be offered to all parties before, during, and after an election and what work the NCSC is doing to preserve the integrity of free and fair elections in the UK overall. This work is vital to defending democracy and providing impartial support. *Our committee therefore requests a private briefing on the preparation that is being put together for an upcoming election and how this support will be provided and delivered.* (Paragraph 66)

10. Cyber insurance can provide a vital lifeline for ransomware victims, offering the sort of support and technical advice not offered by state agencies, as well as driving up cyber security standards through conditions of coverage. Unfortunately, there remains a woeful lack of UK coverage: premiums are unaffordable for many organisations, and have increased drastically in recent years. There are precedents for more extensive Government interventions, where market failures in insurance have wider societal implications. Given the losses endured by ransomware victims and the costs to businesses and public finances, there is a strong economic case for the Government to do more. *The Government should work with the insurance sector to establish a re-insurance scheme for major cyber-attacks, akin to Flood Re, to ensure the sustainability and accessibility of the market.* (Paragraph 72)

11. Victims are currently disincentivised to report ransomware attacks, making it difficult to understand fully the nature and scale of the threat, and how best to tackle it. The Director General of the NCA has suggested that it would be unusual for the Government to require any victim of crime to report an attack—but there are usually greater incentives for reporting of serious crime to take place. The US has also recognised this unique challenge, legislating to mandate reporting by CNI operators. The Government acknowledges that this lack of data creates challenges for the policy response, and experts have told us that it reduces their understanding of how best to protect other organisations against future attacks. *The Government should urgently establish a central reporting mechanism for ransomware attacks, and consider whether to require all UK organisations to report an attack within three months. As part of reporting arrangements, the Government should specify that companies disclose:*

- *Which systems or data have been compromised;*
- *The identity and tactics of the attackers, if known;*
- *Technical details, such as the performance of security and operational systems whilst under attack;*
- *Key details on how the organisation has responded, including communication with secondary victims; and*

- *Which regulators have been notified.*

The data should be kept securely and used for threat intelligence, disruption and prevention work. It could also contribute towards a quarterly, anonymised public report on key ransomware trends. (Paragraph 76)

12. While the Government maintains that UK victims should not pay ransoms, it is the only viable option for many of those directly affected, enabling them to keep their businesses afloat and prevent damaging leaks of personal data. Too many organisational leaders are left to face this moral dilemma alone, without any state intervention. *The NCSC must produce more detailed guidance—accessible to a non-technical audience—on how best to avoid the payment of ransoms after an attack, including negotiating techniques and sources of support for smaller organisations.* (Paragraph 80)

The strategic response — the Government's structures and approach

13. The Government has acknowledged that ransomware is the number one cyber security threat to the UK. It is therefore welcome that it has published an ambitious National Cyber Strategy (NCS), with some strong commitments on resilience and the cyber security of core Government functions, both of which are vital to defending the UK against ransomware. It is also positive that the Cabinet Office has identified the Deputy Prime Minister as holding ministerial responsibility for the National Cyber Strategy, and that there is a cross-government steering group of senior officials to drive delivery work on ransomware. This is a better state of affairs than we have uncovered for some other cross-Government security risks. Nevertheless, there is still a lack of emphasis on prevention and a clear understanding of preventative measures. We remain concerned by the lack of cross-government ministerial fora for overseeing NCS implementation, given the National Security Council's very wide remit and limited schedule of meetings. *The Government should establish an NSC sub-committee on the National Cyber Strategy, which should consider progress against each of the five 'pillars' at least twice per year.* (Paragraph 91)

14. The National Audit Office (NAO) criticised previous delivery failures in cyber security in 2019, finding that the Government risked making the same mistakes with its subsequent National Cyber Strategy. The Government's Performance Framework for the 2022 NCS appears to be a reasonably rigorous approach to monitoring delivery, but its latest Progress Report sheds little light on whether it will achieve the NCS's ambitious objectives, particularly on disrupting and deterring offenders. Given the criticality of the NCS to the UK's national security and prosperity, it is vital that the Government's progress in implementing the NCS is exposed to external scrutiny. *We recommend that the NAO reviews the Government's progress in implementing the National Cyber Strategy through the National Cyber Programme and associated departmental activities, and the effectiveness of the NCS Performance Framework at monitoring and driving delivery.* (Paragraph 92)

15. It is potentially concerning that the Conflict, Stability and Security Fund (CSSF) has now been merged with the National Cyber Programme—which delivers aspects of the National Cyber Strategy—as part of the new Integrated Security Fund (ISF). We recognise that this could encourage a more integrated approach to the UK's

domestic and international cyber work, enhancing our allies' resilience against ransomware actors and addressing threats to the UK's critical supply chains. Given the wide remit of the ISF, however, there is also a risk that cyber work could be deprioritised against other security objectives, at a vital time for the UK's active engagement on cyber security with our international partners. Funding for overseas work also risks being diverted towards domestic priorities, in the face of political pressures closer to home—a risk that we also highlighted in our recent report on the CSSF. (Paragraph 95)

16. *To ensure ongoing transparency and accountability, the Government's Annual Progress Report on the National Cyber Strategy should remain distinct from any Annual Report on the Integrated Security Fund, and should specify how the Government is using ISF funding to deliver NCS objectives. Through its Annual Report and statements to Parliament on the ISF, the Government should continue to make clear the regional, programmatic and thematic allocations for the Fund, as it has done for the CSSF. Finally, as recommended in our recent report on the CSSF, the Government should similarly maintain the CSSF's current levels of transparency in the publication of information on programme activity, spend and performance.* (Paragraph 96)

17. The Home Office claims the lead on ransomware as a national security risk and policy issue, but the then Home Secretary, Suella Braverman MP, showed no interest in it. According to some observers, clear political priority is given instead to other issues, such as illegal migration and small boats. We recognise the significance of illegal migration as a policy challenge, but there is a risk that ransomware is relentlessly deprioritised. The Department's ransomware 'sprint' in 2022 resulted in no discernible policy outcomes. The Minister for Security's acknowledgement of how out of date the Computer Misuse Act is does not excuse the lack of progress which has been made to legislate in this space. It has been two-and-a-half years after its main consultation and 33 years since that dated legislation received Royal Assent. It is hard to see how the Criminal Justice Bill brought forward by the King's Speech 2023 will sufficiently cover the gap left by the outdated CMA. (Paragraph 101)

18. *In line with many other aspects of cyber security, and to ensure that it is treated as a cross-government national security priority, responsibility for tackling ransomware should be transferred from the Home Office to the Cabinet Office, in partnership with the NCSC and NCA. It should also be overseen directly by the Deputy Prime Minister, as part of a holistic approach to cyber security and resilience.* (Paragraph 102)

Raising the costs for attackers — who pays?

19. The National Crime Agency is locked in an uphill struggle against the ransomware threat, which is now so sophisticated that even the most highly-protected organisations expect to experience a ransomware attack. There is clear value in the Government's resilience work, but it is vital that this is paired with further work to raise the costs for attackers, to make the UK a less attractive target. Based on the evidence we have seen, the NCA has insufficient resources and capabilities to match the scale of this challenge. (Paragraph 112)

20. It is possible to infiltrate and disrupt ransomware groups' infrastructure without arresting the criminals involved, sometimes even preventing attacks after the initial

infiltration has taken place. The NCA has some offensive capabilities, but it is vital that the UK is able to operate on a level footing with its international partners. *The Government should invest significantly more resources in the NCA's response to ransomware, enabling it to pursue a more aggressive approach to infiltrating and disrupting ransomware operators.* (Paragraph 113)

21. The NCA's resourcing challenges are exacerbated by the Government's failure to allow them to offer salaries that might attract those with specialist skills. It will always be difficult for the NCA to compete with the private sector, particularly for roles requiring high-level cyber skills, but it is unacceptable that NCA officers are paid less than their policing counterparts. As the elite national squad for serious and organised crime, the public would rightly expect the NCA to offer a competitive pay package, in recognition of the more specialist skills required for defending the UK against serious organised crime. *The Home Office and Treasury should urgently revisit the funding available for NCA pay and progression, which has been an obstacle to achieving pay parity between police forces and NCA officers.* (Paragraph 114)

22. The Government and NCSC's approach to ransomware is often framed through the language of state threats. While we recognise that operators are often facilitated by the Russian harbour state, ransomware is primarily a problem of criminality for profit, rather than espionage or geopolitical sabotage. Through the 2021 Integrated Review and its 2023 Refresh, the Government has acknowledged that the blurred lines between state threats and serious and organised crime require more threat-agnostic capabilities—and yet ransomware is currently at risk of falling into a 'no man's land' between state threats and criminality. (Paragraph 119)

23. Given the links between ransomware crime and certain state actors, it is striking how little attention has been paid to the potential for international law to target the collusion of states. In Chapter 2, our report highlights the possibility that Russia's approach could constitute a violation of international law. *Recognising that Russia shows little, if any, respect for international law, the FCDO should nevertheless investigate the possibilities for legal sanctions and international cooperation to deter state-linked ransomware crime.* (Paragraph 120)

24. The Government's response to ransomware is conducted partly through the National Cyber Force and the intelligence agencies, on which we can only access limited information. RUSI has argued that the UK intelligence community may not be sufficiently motivated or resourced to tackle ransomware, but it is vital that the NCA's work is properly supplemented by the other agencies. *In light of these concerns, and to ensure full scrutiny of state capabilities on ransomware, we recommend that the Intelligence and Security Committee scrutinises the extent and nature of the resources and capabilities devoted to disrupting ransomware operatives by the intelligence agencies, as opposed to combating broader state-sponsored cyber threats. We also recommend that the Committee examines how the intelligence agencies work in partnership with the NCA to deploy a full-spectrum response to the ransomware threat, as envisaged by the Integrated Review and IR Refresh, and how this compares with the US agencies' 'full statecraft' approach to ransomware.* (Paragraph 121)

25. Crypto-assets are the lifeblood of the ransomware ecosystem, and have been a major driver of the increased threat. The Government is making welcome reforms to the

UK's legislative regime underpinning crypto-asset seizure, but we have heard that the NCA has insufficient capacity and skills to make full use of its existing powers, which might be why its total crypto seizures decreased by over a third between 2021/22 and 2022/23. It is essential that the UK bears down on the vast profits of these criminal groups. *The Government and NCA must prioritise further resources towards the training and recruitment of officers with skills in crypto-asset trace and seizure, to reduce the incentives for criminals and to claw back some of the financial losses experienced by ransomware victims.* (Paragraph 125)

26. The UK's main legislative framework on cybercrime is over 30 years old. In that time, the country's relationship with the online world has changed beyond recognition, along with the scale and nature of cybercrime. Rather than introducing a Bill, however, the Home Office has run a second consultation on its proposed reforms to the Computer Misuse Act 1990 (CMA), and only published an analysis on 14 November 2023. We are disappointed that the King's Speech 2023 did not include the CMA and we are still unclear as to how the Criminal Justice Bill is a suitable replacement. *The Government should urgently bring forward legislation to reform the Computer Misuse Act, including to:*

- *Criminalise the theft and copying of data, to bring it in line with property theft offences;*
- *Introduce appropriate extra-territorial provisions for cybercrime;*
- *Give authorities the power to preserve data, pending a decision on formal seizure;*
- *Enable law enforcement agencies to seize domain name and IP addresses; and*
- *Increase the maximum sentences for more serious CMA offences.* (Paragraph 129)

27. There is a high risk that the Government will face a catastrophic ransomware attack at any moment, and that its planning will be found lacking. In 2020, this Committee examined the Government's preparations for the Covid-19 pandemic, considering what it could teach us about how to prepare for a known risk with a high potential impact. We found that the Government had not prepared adequately for a pandemic, despite knowing that there was an increasing chance of such a scenario occurring. The Government is at risk of making the same mistake again: it knows that the possibility of a major ransomware attack is high, yet it is failing to invest sufficiently to prevent catastrophic costs later on. There will be no excuse for this approach when a major crisis occurs, and it will rightly be seen as a strategic failure. If the UK is to avoid being held hostage to fortune and avoid electoral interference it is vital that ransomware becomes a more pressing political priority, and that further substantial resource be devoted to tackling this pernicious threat to the UK's national security. (Paragraph 130)

Formal minutes

Monday 4 December 2023

Members present

Margaret Beckett MP, in the Chair

Richard Graham MP

Lord Strasburger

Lord Butler of Brockwell

Lord Dannatt

Viscount Stansgate

Stephen McPartland MP

Baroness Fall

Lord Robathan

Lord Sarfraz

Robert Courts MP

Ransomware

Draft Report (*A hostage to fortune: ransomware and UK national security*), proposed by the Chair, brought up and read.

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

Paragraphs 1 to 130 read and agreed to.

Summary agreed to.

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

Ordered, 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.

Adjournment

Adjourned till Monday 11 December at 4.15 pm.

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Monday 28 November 2022

Professor Sadie Creese, Professor of Cyber Security, University of Oxford; **Ollie Whitehouse**, Chief Technical Officer, NCC Group; **Jayan Perera**, Principal - Cyber Incident Response, Cyber and Digital, Control Risks Q1–14

Monday 30 January 2023

Sarah Stephens, Managing Director, International Head of Cyber and UK Cyber Practice Leader, Marsh Speciality; **John Ward**, Interim Chief Technology and Transformation Officer, Health Service Executive (HSE) of Ireland; **Councillor Mary Lanigan**, Leader, Redcar and Cleveland Borough Council Q15–34

Monday 24 April 2023

John P. Carlin, Partner, Cybersecurity & Data Protection practice, Paul, Weiss, Rifkind, Wharton & Garrison LLP; former acting US Deputy Attorney General; **Aidan Larkin**, CEO, Asset Reality; **Jamie MacColl**, Research Fellow – Cyber, RUSI; **Emily Taylor**, CEO, Oxford Information Labs Limited; Associate Fellow, Chatham House Q35–52

Monday 19 June 2023

Graeme Biggar, Director General, National Crime Agency; **Rob Jones**, Director General of Operations, National Crime Agency Q53–66

Wednesday 15 November 2023

Rt Hon Oliver Dowden MP, Deputy Prime Minister and Chancellor of the Duchy of Lancaster, Cabinet Office; **Rt Hon Tom Tugendhat MP**, Minister of State (Minister for Security), Home Office; **Lindy Cameron**, Chief Executive Officer, National Cyber Security Centre Q67–85

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

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

1 (ISC)^2 (RAN0010)

2 ACAMS (RAN0030)

3 Association of British Insurers (ABI); and International Underwriting Association of London (RAN0021)

4 BAE Systems (RAN0014)

5 BSI Group (RAN0015)

6 Cabinet Office (RAN0040)

7 Cabinet Office (RAN0018)

8 Carlin, John P. (Partner, Cybersecurity & Data Protection practice, Paul, Weiss, Rifkind, Wharton & Garrison LLP) (RAN0038)

9 Chainalysis Inc. (RAN0008)

10 CrowdStrike (RAN0017)

11 Cyber-SHIP Lab, University of Plymouth (RAN0016)

12 CyberUp Campaign (RAN0003)

13 DXC Technology (RAN0035)

14 FTI Consulting LLP; and Clifford Chance LLP (RAN0034)

15 JUMPSEC (RAN0009)

16 Jones, Mr Andrew (RAN0002)

17 Local Government Association (RAN0024)

18 MacColl, Jamie (Research Fellow - Cyber, RUSI) (RAN0037)

19 Mott, Dr Gareth (Lecturer, Institute of Cyber Security for Society (iCSS), University of Kent); Turner, Sarah (PhD Researcher, Institute of Cyber Security for Society (iCSS), University of Kent); and Nurse, Dr Jason (Senior Lecturer, Institute of Cyber Security for Society (iCSS), University of Kent) (RAN0031)

20 NCC Group (RAN0012)

21 National Crime Agency (RAN0041)

22 National Crime Agency (RAN0039)

23 Norton Rose Fulbright LLP (RAN0028)

24 Orange Cyberdefense (RAN0029)

25 Palo Alto Networks (RAN0033)

26 PlatinumHIT (RAN0026)

27 PwC UK (RAN0006)

28 Queen Mary University of London (RAN0027)

29 Renukappa, Dr Suresh (Senior Lecturer, University of Wolverhampton); Erriadi, Miss Wahiba (Researcher, University of Wolverhampton); Suresh, Dr Subashini (Reader, University of Wolverhampton); and Seabright, Mr Luke (Researcher, University of Wolverhampton) (RAN0011)

30 Renukappa, Dr Suresh (Senior Lecturer, University of Wolverhampton); Subbarao, Mr Chandrashekar (Researcher, University of Wolverhampton); and Suresh, Dr Subashini (Reader, University of Wolverhampton) (RAN0013)

31 Royal United Services Institute (RAN0032)

32 STORM Guidance Limited (RAN0001)

33 Secureworks (RAN0036)

34 Shillito, Dr Matthew (Lecturer in Law, University of Liverpool) (RAN0025)

35 Thales (RAN0019)

36 techUK (RAN0023)

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.

Session 2023–24

Number	Title	Reference
1st Special	The Conflict, Stability and Security Fund: Government Response to the Committee's Second Report of Session 2022–23	HC 349

Session 2022–23

Number	Title	Reference
1st	Readiness for storms ahead? Critical national infrastructure in an age of climate change	HC 132
2nd	The Conflict, Stability and Security Fund	HC 1389
1st Special	Readiness for storms ahead? Critical national infrastructure in an age of climate change: Government response to the Committee's First Report of Session 2022–23	HC 1181

Session 2021–22

Number	Title	Reference
1st	The UK's national security machinery	HC 231
1st Special	The UK's national security machinery: Government Response to the Committee's First Report of Session 2021–22	HC 947

Session 2019–21

Number	Title	Reference
1st	Biosecurity and national security	HC 611
1st Special	Biosecurity and national security: Government Response to the Committee's First Report of Session 2019–21	HC 1279