House of Commons
House of Lords

Joint Committee on the National Security Strategy

# A hostage to fortune: ransomware and UK national security: Government Response to the Committee's First Report

## Second Special Report of Session 2023–24

*Ordered by the House of Commons to be printed 26 February 2024*

*Ordered by the House of Lords to be printed 26 February 2024*

**HC 601**
**HL Paper 74**
Published on 11 March 2024
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 Browne of Ladyton (*Labour*)

Lord Butler of Brockwell (*Crossbench*)

Baroness Crawley (*Labour*)

Lord Dannatt (*Crossbench*)

Baroness Fall *(Conservative)*

Lord Robathan *(Conservative)*

Lord Sarfraz *(Conservative)*

Lord Snape *(Labour*)

Viscount Stansgate (*Labour*)

Baroness Tyler of Enfield (*Life Peer*)

House of Commons

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

Sarah Atherton MP (*Conservative, Wrexham*)

Rt Hon Liam Byrne MP (Labour, Birmingham, Hodge Hill)

Sarah Champion MP (*Labour, Rotherham*)

Richard Graham MP (*Conservative, Gloucester*)

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

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*)

Rt Hon Sir Jeremy Quin MP (*Conservative, Horsham*)

Bob Stewart MP (*Independent, Beckenham*)

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

Mr Robert Courts was a JCNSS member until 27 February 2024, when he was discharged from the Committee.

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

Lord Reid of Cardowan was a JCNSS Member until 31 January 2024, when he was discharged from the Committee.

Lord Strasburger was a JCNSS Member until 31 January 2024, 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 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 the Ransomware 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

# Second Special Report

The Committee published its First Report of Session 2023–24, A hostage to fortune: ransomware and UK national security (HC 194, HL Paper 23), on 13 December 2023. The Government's response was received on 9 February 2024 and is appended to this report.

# Appendix: Government Response

1. The Government is grateful to the Joint Committee on the National Security Strategy for their inquiry into the ransomware threat. We regard ransomware as a serious national security threat and one of the most significant cyber threats facing the UK.

2. Cyber threats have been a consistent priority for the Government since at least 2011 when we published the first comprehensive UK cyber security strategy. The National Cyber Strategy 2022 sets out how the UK will continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in the rapidly evolving online world. It is supported by more than £2.6 billion of investment over three years with a particular emphasis on improving the government's own cyber security. This is in addition to the budget for the National Cyber Force. It is a substantial increase when compared to the £1.9 billion over the five years of the previous strategy.

3. Ransomware is a complex and evolving cyber threat that requires a broad and multi-faceted response from policymakers, law enforcement, intelligence services, industry, civil society and international partners. In the National Cyber Strategy, we said we would, 'review the government's policy and operational approach to tackling ransomware, adopting this as one of our priority campaigns, collaborating with industry and our international partners.'

4. As this report highlights, we have taken a number of steps to raise the cyber resilience of the UK, particularly in government and our critical national infrastructure, while also joining forces with our allies to pursue the criminal groups who conduct ransomware attacks.

5. Below, we have set out the UK Government's response to the individual recommendations made by the Committee.

## Strengthening our defences – UK preparedness and resilience

Conclusion: **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.**

Recommendation: ***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 do not believe that a single, national regulator would deliver improved oversight of NIS sectors, beyond that which the existing multiple regulator approach can deliver. When the UK implemented the original EU Directive, the question of whether to use a single, national regulator for cyber security or, instead, use multiple, sector-based regulators was examined. Supported by feedback from industry, it was agreed that a multiple, sector-based, regulatory system was the best approach. Through this, regulators from specific sectors would have the opportunity to use their knowledge to improve the cyber resilience of individual sectors in a way that a single, national regulator could not. What is appropriate for one sector may not be appropriate for another. We continue to keep regulatory arrangements under review however, and agree that it is vital for regulators to have the capabilities they need to fulfil their roles.

7. For critical national infrastructure (CNI) sectors, security and resilience are overseen by a lead government department that works closely with their corresponding regulators and regulated entities on all elements of resilience and security. This includes ensuring that a CNI cyber remit is included in their governance groups and forums, as well as implementing guidance, legislation and regulatory processes. These cover assurance, inspection and enforcement to ensure that the CNI sector has the appropriate resilience and preparedness to cyber threats.

8. The most recent post-implementation review of the Security of Network & Information Systems Regulations (NIS) Regulations in 2022 identified some of the key challenges faced by both regulators and regulated entities. For regulators, these were primarily around capability and limitations in the regulations themselves, preventing some regulators from making full use of their powers. The Department for Science, Innovation and Technology (DSIT) is focusing its resources to address these issues.

9. Regulators are independent and responsible for implementation in their sector. However, in May 2023 DSIT launched a Monitoring and Evaluation Framework to evaluate the overall effectiveness of NIS implementation on an annual basis. This first round has set a benchmark and will be used to assess progress in the future. DSIT is also undertaking a comprehensive needs analysis of regulator capability, skills and resources, and host inter-regulator engagement and coordination to encourage consistent and complementary regulatory activity.

10. The National Cyber Security Centre (NCSC) provides technical support to the regulatory community and is partnering with regulators to define quality standards for commercially provided services that will significantly augment CNI regulator capacity. Such standards will build on the cyber skills-related work of the UK Cyber Security Council, defining chartered cyber professional status. Some CNI cyber regulators make good use of commercial providers to supplement their in-house capability and there is scope to expand this.

11. To address the limitations in the regulations, in 2022 the Department for Digital, Culture, Media and Sport (DCMS) conducted a public consultation on proposals to improve the NIS Regulations and published a response setting out necessary interventions to improve regulations and enable regulators to make full use of the powers available to them.

12. The Government is committed to delivering these changes as soon as parliamentary time allows and will continue reviewing the implementation of the NIS Regulations.

Conclusion: **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.**

Recommendation: ***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)

13. The frequent testing of readiness and response plans in CNI sectors is an important part of meeting the objectives set out in the National Cyber Strategy 2022. As part of the reinvigorated Cabinet Office-led National Exercising Programme (NEP), lead government departments manage these exercises for their sectors and design and deliver these across areas of risk, working with relevant partners and sectors. The Cabinet Office is currently exploring how to test responses to major cross-cutting risks which impact these sectors.

14. The Cabinet Office, jointly with NCSC, has established a cyber exercising coordination group with representation from across government. The initial objective is to ensure improved visibility of cross-government cyber exercising plans, with the longer-term aim of providing greater strategic direction to exercising programmes by identifying gaps and opportunities for collaboration.

15. Cross-cutting insights from exercises are centrally captured and embedded across lead government departments through the cross-government Training and Exercising Board. The Cabinet Office will continue to publish a Lessons Digest, hosted on the Emergency Planning College's website, which is accessible to the UK resilience community. It complements existing mechanisms for identifying and implementing lessons.

16. The Cabinet Office will also publish and share guidance this year on exercising good practice and managing lessons learned.

Conclusion: **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 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.**

Recommendation: ***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)

17. While local authorities are responsible for the resilience of their networks and systems, the Department for Levelling Up, Housing and Communities (DLUHC) is assigned stewardship of local government resilience. Over the 2021 Spending Review period, DLUHC has been allocated £85.8 million for its Digital Transformation and Cyber Programme for local authorities in England, and this year will introduce the NCSC's Cyber Assessment Framework (CAF) to continue to build a clear and detailed picture of local government cyber risk.

18. The NCSC will continue working collaboratively with DLUHC. In addition to supporting DLUHC's rollout of CAF to local government, the NCSC provide free-of-charge resources to the public sector including early warning and incident response support.

Conclusion: **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.**

Recommendation: ***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)

19. Effective cyber resilience requires both the prevention of cyber-attacks and the ability to recover as quickly and effectively as possible from those that do get through. This requires both the government's and the private sector's support. The NCSC's role in this context is to understand the threat and help others to build their resilience. This includes facilitating an ecosystem where victim organisations can draw on trusted, existing industry resources for recovery and remediation that are tailored to their needs. Cyber Incident Response companies, and similar organisations, are well placed to provide the hands-on activity that is required to support the unique requirements of any given organisation.

20. The Government has also launched the Government Cyber Coordination Centre, also known as the GC3, which brings together cyber defenders from across the government to act as a force multiplier for existing government incident management processes, operational activities and resilience work. It aims to achieve a step change in the coordination of cyber resilience efforts across government and the wider public sector primarily via lead government departments.

21. With regards to establishing a 'pro bono' scheme, there are already some charities and initiatives that seek to provide such support. NCSC has engaged with some of them and will continue to explore this further.

Conclusion: **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.**

Recommendation: ***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)

22. The Cabinet Office will happily provide a briefing for the Committee to discuss preparations for the upcoming election in due course.

Conclusion: **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.**

Recommendation: ***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)

23. The Government recognises the important role that cyber insurance plays in helping to build resilience to cyber-attacks including those which involve the use of ransomware. However, the Government does not generally intervene in insurance markets as this could damage competition in the market.

24. The Government recognises ongoing challenges in the provision of cyber insurance, and our current, primary focus is to support the insurance industry to strengthen and grow the commercial cyber insurance market. For example, the Government worked with the Information Commissioner's Office and the Association of British Insurers to release anonymised cyber breach data to insurers to improve their modelling and help ensure premium prices are risk reflective.

25. Pricing is a commercial decision by insurers, and the respective capabilities of insurers to assess risk is a key element on which they compete. Risk reflective pricing in cyber insurance is particularly important, given its role in encouraging policy holders to engage in preventative measures to improve cyber resilience. As we continue to make progress on the National Cyber Strategy's wider objective of building businesses' cyber resilience, we would expect to see reduced claims and lower premiums for policyholders.

Conclusion: **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.**

Recommendation: ***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)***

26. Under-reporting is a recognised issue in our understanding of the scale of the ransomware threat affecting the UK, and the Government is looking at ways to encourage reporting and uptake of best practices.

27. Action Fraud is the national reporting service for individuals and organisations to report fraud and cyber crimes, including ransomware. We have invested £30 million to replace Action Fraud with a modern system in 2024 to improve ease of reporting and support for victims, with improvements already underway. Through the National Cyber Fund, we have invested in the creation of the Enhanced Cyber Reporting Service to better collect and understand cyber-attacks.

28. The Government shares advice and guidance on GOV.UK, outlining the organisations victims of a ransomware attack can report to. These include Action

Fraud on behalf of law enforcement, the Information Commissioner's Office for any loss of personal data and breaches of the UK GDPR, and the NCSC for the most sophisticated and high-impact attacks.

29. The Government Security Group has focused its cross-government incident coordination processes in the last year to enable a consistent view of incidents and impacts from across government departments. The establishment of GC3 with NCSC late last year further enhanced this process, providing a single front door for government organisations to report incidents to and simplify reporting requirements when a cyber incident is declared.

30. The Government is undertaking further work to increase reporting from organisations, including examining regulatory levers.

Conclusion: **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.**

Recommendation: ***The NCSC must produce more detailed guidance—accessible to a nontechnical 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)

31. The NCSC will continue to update their practical, action-orientated guidance, accessible through the NCSC website, which includes the Ransomware Hub. These updates will pay particular attention to advice for small and medium-sized businesses and are done in collaboration with law enforcement counterparts who have a leading role in supporting victim response. The Government would also welcome increased levels of incident reporting.

32. The NCSC and the NCA will continue to support the Home Office in developing proposals to achieve a reduction in ransom payments.

## Responding to attacks – victim support and recovery

Conclusion: 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.**

Recommendation: ***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)

33. The Deputy Prime Minister provided a comprehensive summary of ministerial oversight of the National Cyber Strategy at the oral evidence session in November. The National Security Council and its existing sub-committees plus the Ministerial Cyber Board, chaired by the Deputy Prime Minister, together provide frequent opportunities for ministers to drive the implementation of the Government's cyber priorities.

34. To further support the delivery of the National Cyber Strategy, the Government has set up the National Cyber Advisory Board (NCAB) which brings together leaders from academia and industry to allow the government to harness networks from across the cyber ecosystem, mobilising them to support delivery across all five pillars of the strategy. The NCAB met most recently with the Deputy Prime Minister in November and again in January with their Japanese counterpart, Keidanren's Cyber Security Committee, where they discussed a number of priority cyber issues, including ransomware and cyber resilience.

Conclusion: **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.**

Recommendation: ***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)

35. As the independent auditor of government, it is for the Comptroller and Auditor-General to decide how to respond to this recommendation. Should work be undertaken in this area by the NAO, the Government will provide any assistance required.

Conclusion: **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)

Recommendation: ***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)

36. The Government remains committed to transparency and accountability, as well as the monitoring and evaluation of activities that support our cyber ambitions. These will continue as an integral part of the Government's Annual Progress Report on the National Cyber Strategy, and we will continue to report as we have done so previously.

37. Similarly, with regard to the Integrated Security Fund, the Government remains committed to transparency and will continue to publish information on regional, programmatic and thematic allocations for the Fund. Most recently, the Government's publication of the CSSF Annual Report FY 22/23 on 16 January 2024 included information on regional and thematic allocations.

Conclusion: **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)

Recommendation: ***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)

38. As the Committee heard in evidence from the Security Minister and Deputy Prime Minister, ransomware is a key security priority for the Home Office and wider Government.

39. The Home Office leads the cross-government ransomware work under the Threat Pillar of the National Cyber Strategy which is overseen by the Deputy Prime Minister, and works very closely with the MoD and FCDO and the wider community, including

law enforcement and the UK intelligence agencies, who also play a significant role in the response to ransomware. There are currently no plans to change this arrangement, and the Home Office remains the lead Department for overall crime.

40. The Home Office chairs the Senior Ransomware Steering Group which drives comprehensive delivery at a senior level across government. The group brings together cross-government policy, intelligence and law enforcement partners, and oversees all recommendations and updates that Ministers receive.

41. The Home Office has boosted law enforcement capabilities through the National Crime Agency and local police forces. They have also launched specialist cybercrime units in every local police force in England and Wales, investing £42 million. They have grown the NCA's National Cyber Crime Unit, increasing their ability to investigate ransomware.

42. The Home Office will continue to lead and coordinate the cross-government ransomware work under the Threat Pillar of the National Cyber Strategy.

## Raising the costs for attackers – who pays?

Conclusion: **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.**

Recommendation: ***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)

43. The Government agrees that the NCA plays a vital part in our response to ransomware and cybercrime. As set out in the new five-year Serious and Organised Crime Strategy, published 13 December 2023, the Government is committed to tackling serious and organised crime in and against the UK. To help achieve this outcome, we have made significant progress in strengthening the NCA: since its formation in 2013, the NCA's workforce has grown by almost 40% and, within the last two FY years alone, the Agency's budget has increased by 21% from £711 million in 2021/22 to over £860 million in FY 2023/24. This investment, alongside the NCA's ongoing portfolio of transformation, will help ensure that the Agency has the digital and physical infrastructure in place to respond to the evolving threat posed by ransomware. The NCA remains an active and committed member of the UK Government's offensive cyber community.

Conclusion: **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.**

Recommendation: ***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)

44. The Government recognises the importance of reforming the NCA's existing pay structure and has been working closely with the Agency to ensure any changes are in its best interest and that of its workforce.

45. The NCA champions a 'One NCA' culture in which the distinction between warranted and non-warranted officers is not a simplistic relationship between operational and non-operational roles. Ensuring that all NCA officers benefit from a uniform pay structure forms a key part of the NCA's long-term workforce strategy and is critical to ensure that all Agency officers are treated equitably when it comes to pay.

46. Alongside this, the Pay Review Bodies process is a well-established one and provides evidence-based advice to the government on levels of pay for their remit groups. In FY 2022/23, all NCA officers received a 5% in remuneration costs uplift, the highest pay award in the Agency's history. The outcome of the 2023–24 NCA pay award will be published shortly. The Home Secretary initiated the process for FY 2024/25 on 20 December 2023, requesting a report from the Pay Review Body by June 2024.

47. We fully recognise that a strong pay framework is vital to the NCA being able to deliver its role in leading the law enforcement system to disrupt and dismantle the most harmful organised crime groups operating in and against the UK.

Conclusion: **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.**

Recommendation: ***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)

48. Russia is one of the most prolific actors in cyberspace and we recognise that their activity has been a significant driver of ransomware threats in the UK.

49. In conjunction with the US, the UK has delivered ransomware sanctions designations, targeting the activity of 18 Russian cyber criminals through two tranches in February and September 2023. These sanctions have significantly hampered the ability of cyber threat actors to monetise their cyber criminal activities.

50. Sanctions are proven to be an effective and potent tool in deterring cyber threats, imposing meaningful costs and signalling that malicious cyber activity has consequences. The UK will continue to use sanctions as a targeted instrument to de-anonymise, sow discord, and impose costs on those who conduct malicious cyber activity. We will also continue to adapt and reinforce our approach, exploring ways in which sanctions can be applied to respond to cybercrime while supporting and building our allies' capabilities to respond and deter the variety of cyber threats we are confronted with. Sanctions are

just one tool which the Government uses, alongside a wide range of policy, diplomatic, operational and law enforcement tools to identify and disrupt cyber-criminal actors and to deter and disrupt Russia's harmful activity.

Conclusion: **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.**

Recommendation: ***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)

51. The Intelligence and Security Committee (ISC) of Parliament has the autonomy to set its own agenda and work programme within the remit established by the Memorandum of Understanding between the Prime Minister and the ISC.

52. The Government has shared the recommendation with the Office of the ISC to ensure they are aware of the Committee's recommendation.

Conclusion: **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.**

Recommendation: ***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)

53. Organised crime is ever evolving and the NCA is a core part of our response to these threats. We agree that it is crucial that the NCA recruits and retains the professional and specialist skills needed to combat malicious online actors.

54. To help the NCA continue to develop the critical capabilities it needs to achieve this, the Agency's budget has increased by at least 21% in the last two years to over £860 million. The Home Office will continue to monitor and review the pay of NCA officers to ensure the Agency is able to attract, recruit and retain the right people, particularly those with technological and digital skills.

55. Alongside this, the Economic Crime Plan 2, published March 2023, sets out the Government's plan to combat criminal abuse of crypto-assets. A critical part of this response is the development of law enforcement training pathways to produce and maintain a pool of highly skilled investigators and intelligence officers, alongside strengthening technological capabilities across the system to help recover more criminal crypto-assets. Specifically, Action 7 in the ECP 2 commits to the establishment of training opportunities for front-line officers, financial investigators, intelligence officers and accredited crypto-asset professionals, to be delivered by the NCA.

Conclusion: **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.**

Recommendation: ***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 12

56. The Government agrees that the Computer Misuse Act is vital in allowing us to take action against those committing cyber-attacks and is essential in enabling us to tackle the threats to our citizens, businesses and public services.

57. As part of the Criminal Justice Bill, we have brought forward measures to create a new power to enable UK law enforcement to suspend domain names and IP addresses that are being used for serious crime. Under the provisions, a UK law enforcement agency will be able to apply for a court order mandating action which they can serve on entities based in the UK and overseas. This will be an important tool in supporting UK Law Enforcement to pursue criminal activity impacting UK citizens and businesses.

58. As the Committee is aware, the Home Office is in the process of reviewing the CMA and the powers available to law enforcement agencies to investigate CMA offences. That review is ongoing and will consider the Committee's recommendations as part of that work.

59. As part of the review, the Home Office also ran a public consultation earlier this year on giving authorities the power to require the preservation of data, targeted at law enforcement, domain name registrars and registries, as well as hosting providers. While the power had broad support, the published 'consultation outcome: analysis of responses' document summarises that concerns were raised about the costs of long-term data storage. The Home Office will, therefore, engage with public and private sector organisations to suitably understand further impacts and look to mitigate them effectively before considering legislation.