UK Parliament POST

POSTNOTE

Number 684 October 2022

States' use of cyber operations

States are increasingly engaging in cyber operations to support their strategic aims. This POSTnote considers hostile state-backed cyber activities. It looks at how and why states use cyber operations against other nations and the threats posed to the UK. It also considers mitigations, both internationally and in the UK.

Overview

- The UK is routinely targeted through cyber operations backed by foreign states.
- Operations may be conducted for political, military or financial gain, and may lead to loss of important data, disruption to critical services, or the spread of false information.
- The UK Government says China and Russia pose the greatest state-backed cyber threat.
- The UK has world-class strengths in cyber security and intelligence, but has shortfalls in its skilled cyber workforce.
- Mitigations against state cyber operations include improving skills, raising basic cyber security, and developing cyber technologies, standards and offensive capabilities.

Background

'Cyberspace' typically refers to digital networks (such as the internet) used to store, modify and communicate information.[1-3] 'Cyber operations' aim to achieve objectives in or via cyberspace. They can include gaining unauthorized access to computers, systems or networks to obtain information; and altering, deleting, corrupting or denying access to data or software.[4] States use cyber operations for reasons including to gather information, influence political decisions, support military action or gain financially.[5-10] They offer new ways of achieving old strategic ends, such as espionage, subversion and sabotage.[1,11,12] Impacts can include data breaches, website outages and disruption to online services and supply chains.[2,7,13,14]

Building a full picture of the cyber operations conducted globally is difficult.[15-17] Victims may not discover a breach for years, and may think that reporting it will cause reputational harm or business disruption.[18-22] Also, states' cyber operations may be sophisticated, covert and designed to be difficult or impossible to attribute.[23] Studies have tried to quantify states' malicious cyber activities. Microsoft analysis of customer security data suggested that in 2020/21 the UK was targeted by 9% of state cyber operations, the third most targeted country behind the US (46%) and Ukraine (19%).[14] Analysis by cyber security firm Crowdstrike of global cyber security threats in 2021, estimated that although the largest proportion of cyber intrusions (49%) were financially motivated criminal operations, at least 18% were by state or state-backed groups.[24]

The number and sophistication of cyber-attacks on the UK are increasing.[14,24,25] In 2020/21, the National Cyber Security Centre (NSCS, Box 1) dealt with 777 incidents (from state and non-state actors), a rise of just over 30% in four years.[26] The UK Government set out plans for protecting and promoting UK interests in cyberspace in the National Cyber Strategy 2022. This included £114m of extra funding for the National Cyber Security Programme to help deliver the strategy over the next three years, which is part of a wider £2.6 bn investment in cyber and legacy IT.[2,27,28] The Government is reviewing the Computer Misuse Act and has introduced the National Security Bill, which may help to strengthen the UK's response to cyber threats from hostile states.[29,30]

Motivations behind states' cyber operations

States may conduct operations through their security and foreign intelligence agencies or via non-state proxies, such as private contractors.[31] Hence, various cybercriminal groups are suspected of sometimes working in the interest of specific nations.[32] Generally, state-backed operations tend to coincide with a geopolitical dispute, may persistently target strategic assets (with operations continuing despite a lack of success), and may be especially sophisticated and resource-intensive.[14,33] However, states also use simple techniques, such as 'phishing' emails that con recipients into sharing sensitive information.[34,35]

The UK Government has stated that China and Russia pose the greatest of state-backed cyber threats to the UK,[2] and that Iran

Box 1: Key UK Government organisations responsible for countering cyber threats

- **National Cyber Security Centre (NCSC)** – the national authority on cyber security in the UK.[2] An arm of the Government Communications Headquarters (GCHQ), it is tasked with improving the UK's cyber defence and resilience. It supports the private and public sectors in threat identification, protection and recovery from attacks.
- **National Cyber Force (NCF)** – a partnership between the MOD, GCHQ, the Secret Intelligence Service (MI6) and the Defence Science and Technology Laboratory. NCF is responsible for carrying out offensive cyber operations to counter the cyber operations of the UK's adversaries.[2,39]
- **National Cyber Crime Unit, National Crime Agency** – provides national leadership and coordination of the UK's response to cyber crime.[40]

The Cabinet Office leads the Government's overall response to cyber threats. The Home Office leads work to detect, disrupt and deter adversaries, alongside the FCDO and the MOD. The Secretary of State for Foreign, Commonwealth and Development Affairs is responsible for GCHQ, and jointly responsible for NCF with the Secretary of State for Defence.

and North Korea also have notable cyber capabilities (Box 2).[14,26,36,37] Typically, states conduct cyber operations to obtain data (espionage),[13] disrupt services,[14] or spread disinformation. Some states commit cybercrime for financial gain.[16] Nations can be affected by cyber operations even if they are not the intended target (see WannaCry and NotPetya attacks, Box 3).[38]

Espionage

According to Microsoft, espionage was the most common goal of state-on-state cyber operations in 2020/21.[14,13] MI5 says that cyber espionage allows hostile actors to steal large volumes of information remotely, cheaply and with relatively little risk to personnel.[1,41] It may also make it easier for states to deny involvement,[42] for example, by using a criminal group to act on their behalf. Data collected through cyber espionage may be used for political or commercial advantage, and government bodies, NGOs and think-tanks are common targets.[14,43] The Home Office says that UK industry, academia, defence and business sectors are also routinely targeted by foreign states.[30] Intellectual property (IP) theft can erode competitive advantage, devaluing companies' products and services.[26,44] The heads of MI5 and the FBI have warned of the threat posed by the Chinese Communist Party, including its use of cyber to steal research and IP.[45,46] The NCSC say that Russia used cyber operations against the UK to steal IP relating to vaccines.[47]

States target managed service providers (MSPs) for espionage. MSPs are third-party firms contracted by other organizations to provide their customers with services, such as legal, human resource,[48,49] or IT services.[24,50,51] A hostile actor may exploit vulnerabilities within MSP products or services to gain access to the MSP's customers; an example of a supply chain attack[52-55] (SolarWinds and Microsoft Exchange, Box 3). Compromising a single MSP can enable access to hundreds of organisations and huge amounts of data.[2,52] Analysis of 115 supply chain attacks and vulnerabilities from 2010-2020, found that almost a quarter came from states.[56] Industry analysts suggest states, especially Russia,[14] are targeting the customers of MSPs more often.[24]

Box 2: States' use of cyber operations

- **Russia** – CrowdStrike reports that Russia mostly uses cyber operations against states for intelligence gathering, and Microsoft says that Russia-based groups are increasingly targeting governments.[2,13-14] The US Office for the Director of National Intelligence (ODNI) reported that Russia also attempts to hack organisations and journalists that investigate Russian Government activity.[57] Disruptive cyber-attacks,[58-62] including against Ukraine and the US energy industry, have been attributed to Russia.
- **China** – Industry research suggests that China-based groups have thus far focused on espionage, intellectual property theft and surveillance; most frequently targeting governments and the healthcare, technology and telecommunications sectors.[2,13,14,63] The ODNI has said that China is almost certainly capable of cyber-attacks that would disrupt US critical infrastructure, and that it conducts cyber operations to counter perceived threats to the Chinese Communist Party, such as hacking journalists.[57]
- **Iran and North Korea** – The UK Government reports that although less sophisticated, Iran and North Korea use digital intrusions to achieve their objectives, including through theft and sabotage.[2] For North Korea, this includes using cyber-attacks to raise funds.[64-68]

Disruption to essential services

Disruption in cyberspace has the potential to cause serious disruption in the physical world (POSTnote 554),[69] including to critical national infrastructure (CNI).[70,71] The NCSC categorises cyber incidents on a scale from 1 to 6. Category 1 refers to a national cyber emergency that causes sustained disruption to essential services or affects national security, leading to severe economic or social impacts, or loss of life. Category 6 attacks are localised incidents, such as an attack on an individual.[72]

States may pre-emptively enter an adversary's network to gain a foothold for a future attack.[34,73,74] Such 'pre-positioning' activities can be hard to distinguish from espionage.[75] In 2018, the NCSC and US Government reported that Russia had potentially conducted 'pre-positioning' activities on CNI in the US and UK.[74,76] In March 2022, the White House warned that the Russian Government was exploring options for potential cyber-attacks on US critical infrastructure in response to economic sanctions imposed on Russia for invading Ukraine.[73]

Cyber operations can be unpredictable and difficult to control, so may affect infrastructure[77] even if it is not the intended target. Factors that can increase the risk of disruption, include:

- **Legacy IT** – older systems and their component software and hardware may no longer receive updates and patches to address security vulnerabilities.[78] A 2022 Cabinet Office report stated that legacy IT can have a significant negative impact on cyber and national security.[79]
- **Supply chain complexity** – infrastructure providers rely on third-parties to supply crucial software and services.[70] Digital supply chains are often large and complex, making it hard for organisations to check fully the cyber security of the products and services they rely on.[46,80] The US Cyberspace Solarium Commission raised concerns that imported components may have vulnerabilities planted or intentionally unaddressed by adversaries.[81] A 2022 Ipsos survey of UK businesses and charities found that most had not formally reviewed their supply chain risks.[82]

- **The Internet of Things (IoT)** – infrastructure providers are increasingly deploying internet-connected devices on their networks, potentially introducing vulnerabilities that might be targeted. This risk is exacerbated by the poor cyber security of many IoT consumer devices (POSTnote 593).[83]

Spreading disinformation

States engage in disinformation operations (that spread deliberately false information) for reasons that include: to achieve political goals without escalation to physical warfare; to influence the international response towards a particular nation;[109-111] or to erode trust, for example in authorities or democracy.[112,113] The EU Agency for Cybersecurity (ENISA) says that there was a rapid rise in disinformation operations during the COVID-19 pandemic.[114] ENISA highlight social media as a key way of spreading disinformation,[115] although it is also spread in other ways, such as by email (POSTnote 559).[116]

International response to cyber operations

The UK is recognised as having world-class strengths in cyber security and cyber intelligence, and clear strategic oversight at the political level, according to a comparison of 15 states by the International Institute for Strategic Studies.[21,117] It noted shortfalls in the UK's skilled cyber workforce, an inability to invest on the same scale as the US and China, and a lack of an industrial base to build and export equipment that may help to shape the future of cyberspace. The study concluded that some shortfalls are partly offset by the UK's international alliances.

International defence and security partnerships

The UK participates in international partnerships to share intelligence, best practice and cyber capabilities.[117] These include bilateral relationships (such as with the US), the Five Eyes intelligence sharing alliance (the US, Australia, Canada, New Zealand and the UK), and NATO.[118,119] NATO facilitates information sharing and assistance between allies to prevent, mitigate and recover from cyber-attacks.[120-123] The UK has offered its offensive cyber capabilities (see page 4) in support of agreed NATO goals.[124] In 2019, the Secretary General of NATO stated that a serious cyber-attack could trigger NATO's collective defence commitment, where an attack against one ally is treated as an attack against all.[125]

Establishing international laws and norms

It is broadly accepted that existing international law (such as the Hague and Geneva conventions) applies in cyber-space.[31,126,127] NATO's Tallinn manuals are advisory, non-binding documents that provide expert opinion on how aspects of international law can be applied to cyberspace.[128,129] They conclude that states can respond in self-defence to cyber operations that cross the threshold of armed conflict,[128,130] however, the vast majority to date have fallen below this.[131]

Accepted norms may help the international community to hold accountable those who operate outside "acceptable" behaviour, and inform decisions about proportionate responses.[132] However, there is debate about their efficacy. [126,129,133-142] The UK participates in various state-led groups that aim to establish norms, including the UN Open-Ended Working Group,[143] the Organisation for Security and Co-operation in Europe,[144,145] and standards bodies such as the European Telecommunications Standards Institute.[146,147] Industry groups also seek to influence norms through initiatives such as the Cybersecurity Tech Accord and the Global Commission on the Stability of Cyberspace.[148-153]

Box 3: Examples of suspected state-backed attacks

- **Bronze Soldier (2007)** – Distributed denial-of-service (DDoS) attacks blocked access to Estonian Government, media and bank websites by flooding them with requests. This followed a decision to move a Soviet memorial.[84,85]
- **Stuxnet (2010)** – The first targeted cyber-attack on an industrial control system. Widely attributed to the US and Israel as an attack on Iran's nuclear capabilities.[86-89]
- **WannaCry (2017)** – Ransomware attack, likely by North Korea, affecting 300,000 computers in over 150 countries. Unintended victims included 48 NHS trusts, leading to estimated losses of £35 m and 19,000 cancelled appoint-ments.[90-93]Ransomware typically renders files inaccessible by encryption and demands a ransom to restore them.[94]
- **NotPetya (2017)** – Cyber-attack on Ukraine's financial, energy and public sectors that irreversibly encrypted computer files. It affected governments, businesses, hospitals and others globally, with losses estimated at over $10 bn (£8.9 bn). Attributed to Russia.[95-98]
- **SolarWinds (2020)** – Cyber intrusion operation carried out via a supply chain compromise of IT management software from SolarWinds.[99] Impact on the UK was low, but 18,000 organisations were affected globally. Attributed to Russia.[26,100]
- **Microsoft Exchange (2021)** – Large-scale industrial espionage attack exploiting vulnerabilities in Microsoft's email and calendar hosting program. The EU reported significant economic losses for government institutions and companies.[101] Attributed to China.[101-104]
- **ViaSat (2022)** – A DDoS attack on global satellite communications company, ViaSat, on the day Russia invaded Ukraine.[105] ViaSat said that this affected several thousand customers in Ukraine and tens of thousands of others across Europe.[105-107] Attributed to Russia.[108]

Attribution and sanctions

States and companies may attribute a cyber operation to a nation or group they assess to be responsible and, in some cases, announce this publicly.[2,91,103,154-157] Motivations for public attributions include apprehending attackers (if possible), deterring future attacks, and highlighting unacceptable behaviours to reinforce norms.[135,158,159] States typically offer few details with attributions.[154,160-162] However, detailed evidence may be published alongside indictments, such as those filed by the US Department of Justice in 2022 against Russian Federal Security Service agents for cyber operations targeting oil refineries, nuclear facilities and energy companies.[163-165]

States are sometimes sanctioned for cyber operations, such as the EU's sanctions against Russia in 2019 after the NotPetya attack (Box 3).[96,166,167] The UK Government says that attribution is a critical part of deterring cyber threats.[2] However, some analysts question the efficacy of deterrence, including through attributions and sanctions.[13,77,131,134-136,158,168-172]

Mitigating cyber operations in the UK

The National Cyber Strategy sets out the Government's approach to counter cyber threats and increase resilience to attacks (Box 1). Aims include averting attacks, abating the effects of attacks that do occur, and enabling fast recovery.[173]

Here, we consider aspects most relevant to the threats from hostile states. These include developing offensive cyber capabilities, raising levels of basic cyber security, improving the resilience of critical infrastructure, growing the cyber workforce, and developing cyber-related technologies and standards.[2]

Offensive cyber capabilities

The National Cyber Strategy defines offensive cyber operations (OCOs) as the adding, deleting or manipulating of data on systems or networks to deliver a physical, virtual or cognitive effect (for example, changing opinions).[9,90] The Government says that OCOs by the National Cyber Force (Box 1) could include: degrading adversary weapons systems, disabling terrorist communications and countering state disinformation.[2] The MOD and GCHQ say they used OCOs against Daesh (also known as Islamic State) to hinder its ability to spread propaganda and coordinate attacks, and to protect coalition forces on the battlefield.[67,175] There may be legal and ethical constraints when using OCOs.[136,176] Their effectiveness as deterrents may also be limited if, unlike other types of deterrent such as nuclear weapons, it is not clear what OCO capabilities an adversary has.[177]

Improving basic cyber security

Microsoft estimates that basic cyber security practices could prevent 98% of attacks (from state and non-state actors),[14] but they will not stop the most sophisticated attacks.[67,178] Industry, academia, governments and non-profit organisations[151,179-181] are involved in initiatives to help improve the cyber security of individuals, organisations, devices and online services.[2,178] Here we focus on UK Government activities, which include:

- **Product Security and Telecommunications Infrastructure Bill** – aims to create mandatory security standards for internet-connectable consumer devices.[182,183]
- **National Security Bill** – aims to reform existing counter-espionage laws, including new offences to tackle state-backed sabotage, foreign interference, theft of trade secrets and the assistance of foreign intelligence services. (Commons Library briefing CBP-9559).[30,184-186]
- **Online Safety Bill** – aims to require companies (such as social media platforms) to address potentially harmful content, including disinformation.[187,188]
- **National Security and Investment Act 2022 (NSI)** – the NSI gives the government powers to intervene in business acquisitions that could harm UK national security. For example, if companies manufacture computing hardware or form part of a telecommunications digital supply chain.[189]
- **Review of the Computer Misuse Act 1990 (CMA)** – the CMA is the main piece of legislation regarding computer-dependent crime. The Home Office is reviewing whether it adequately covers the harms included in the remit of the Act, such as whether law enforcement agencies have the necessary powers to deal with CMA offences, and if the CMA is fit for use in light of technological advances since 1990.[29]
- **Cyber Security Incentives and Regulation Review** – DCMS reviewed progress in improving UK cyber resilience from 2016 to 2021. The Government said it was considering ways to mandate large companies to address cyber risks.[178]
- **Cyber Essentials scheme** – offers advice and tools to organisations to protect against common types of cyber-attack.[190,191] The Government has said it will look at ways to increase uptake, which is currently low.[178,192]
- **Active Cyber Defence programme** – aims to tackle common, unsophisticated attacks.[193] Activities include taking down malicious websites, giving warnings of possible attacks, and creating tools to test organisations' cyber defences.[194]
- **Attack detection** – the NCSC and the Alan Turing Institute are exploring whether machine learning (POSTnote 633) can detect some cyber-attacks.[2]

Improving the resilience of critical infrastructure

Much of UK CNI is privately owned, operated and maintained.[195-199] In 2018, the Joint Committee on the National Security Strategy highlighted UK CNI cyber security weaknesses including supply chain vulnerabilities, a lack of political leadership, and a skills shortage.[70] In particular, they found a lack of expertise related to the security implications of connecting bespoke or legacy CNI to the internet.[200] The Network and Information Systems (NIS) Regulations 2018, require CNI operators and relevant digital service providers to implement cyber security improvement measures.[52] A DCMS review reported that the regulations were improving CNI security but that further improvements were required, for example in areas such as supply chain cyber security.[52,115,201,202] Thus, DCMS has proposed extending the NIS regulations to cover MSPs[203] and a wider range of sectors,[178] and to require large companies to report all cyber-attacks to regulators (not just those affecting services).[203]

Developing the specialist cyber workforce

The UK cyber security workforce grew by around 50% from 2018 to 2022, but demand for skills still outstrips supply.[2,203-205] In 2022, DCMS estimated that about 51% of UK businesses had a basic skills gap.[206] Enhancing the UK's cyber skills is a key Government objective, as is improving diversity in the cyber workforce.[2,207,208] It launched the UK Cyber Security Council in 2021, a professional body for the UK's cyber security workforce, tasked with creating consistency across standards, career path-ways, and certification to recognise competent individuals.[209]

Developing digital technologies and standards

Developing standards can help to increase cyber security,[210] for example by facilitating the sharing of knowledge and best practice, and providing a basis for comparing the security of different products.[211] Technology and standards development can bring economic benefits and geopolitical influence. The US Cyberspace Solarium Commission (CSC) cites China's 5G technology (POSTbrief 32) development as an example of this.[158] The Chinese state invested heavily in research and development[81] and co-ordinated with industry on early 5G standards,[212] helping China to become a leading exporter of 5G technologies.[213,214] The CSC has raised concerns that international technical standards are being increasingly informed by the authoritarian values and policies of the Chinese Government.[158] The National Cyber Strategy aims to reduce UK reliance on non-allied states for digital technologies, to avoid security risks. It says that the Government will work with stakeholders to shape global digital technical standards to uphold democratic values, ensure cyber security and advance UK strategic interests.[2]

References

1. MI5 (2016). Introduction to Cyber. *MI5 Security Service*.
2. UK Government (2022). National Cyber Strategy 2022.
3. Computer Security Resource Center Glossary - Cyberspace. *NIST*.
4. Dinstein, Y. *et al.* (2020). Section II: Cyber Operations. in *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary*. (eds. Dinstein, Y. et al.) 19–29. Springer International Publishing.
5. Valeriano, B. *et al.* (2015). Cyber War versus Cyber Realities: Cyber Conflict in the International System - Oxford Scholarship. Oxford University Press.
6. Voo, J. *et al.* (2020). Reconceptualizing Cyber Power.
7. ENISA (2021). ENISA Threat Landscape 2021. *ENISA*.
8. Smeets, M. (2018). A matter of time: On the transitory nature of cyberweapons. *Journal of Strategic Studies*, Vol 41, 6–32. Routledge.
9. Taillat, S. (2019). Disrupt and restraint: The evolution of cyber conflict and the implications for collective security. *Contemporary Security Policy*, Vol 40, 368–381. Routledge.
10. Harknett, R. J. *et al.* (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, Vol 0, 1–34. Routledge.
11. Rid, T. (2013). *Cyber War Will Not Take Place*. Hurst.
12. Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, Vol 35, 5–32. Routledge.
13. Crowdstrike (2021). 2021 Global Threat Report.
14. Microsoft (2021). Microsoft Digital Defense Report.
15. Centre for Strategic and International Studies (2022). Significant Cyber Incidents. *Centre for Strategic and International Studies*.
16. Carnegie Endowment for International Peace (2022). Timeline of Cyber Incidents Involving Financial Institutions. *Carnegie Endowment for International Peace*.
17. Neto, N. N. *et al.* (2021). Developing a Global Data Breach Database and the Challenges Encountered. *J. Data and Information Quality*, Vol 13, 1–33.
18. Tsukayama, H. (2016). It took three years for Yahoo to tell us about its latest breach. Why does it take so long? *Washington Post*.
19. Swinhoe, D. (2019). Why businesses don't report cybercrimes to law enforcement. *CSO Online*.
20. DCMS (2021). Cyber Security Breaches Survey 2021. UK Government.
21. Voo, J. *et al.* (2020). National Cyber Power Index 2020. Belfer Centre.
22. CrowdStrike (2022). Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign. *crowdstrike.com*.
23. Ilker, K. (2021). Cyber-Espionage Malware Attacks Detection and Analysis: A Case Study - The University of Sheffield. *Journal of Computer Information Systems*,
24. CrowdStrike (2022). 2022 Global Threat Report.
25. Capstone Partners (2021). Increased Sophistication of Cyber Attacks Heightens Demand.
26. NCSC (2021). NCSC Annual Review 2021. NCSC.
27. HM Treasury (2021). Autumn Budget and Spending Review 2021.
28. National Audit Office (2019). Cabinet Office Progress of the 2016-2021 National Cyber Security Programme. National Audit Office.
29. Home Office (2021). Call for Information: Computer Misuse Act 1990. Home Office.
30. Home Office (2021). Legislation to counter state threats. UK Government.
31. Boeke, S. *et al.* (2018). The Demilitarisation of Cyber Conflict. *Survival*, Vol 60, 73–90. Routledge.
32. Mandiant (2022). Advanced Persistent Threat Groups. *Mandiant*.
33. Thomas, M. A. (2022). Distinguishing Cyberattacks by Difficulty. *International Journal of Intelligence and CounterIntelligence*, Vol 0, 1–22. Routledge.
34. U.S. Department of the Treasury (2020). Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware. *U.S. Department of the Treasury*.
35. Bossetta, M. (2018). The Weaponization of Social Media: Spear Phising and Cyberattacks on Democracy. *Journal of International Affairs*, Vol 71, 97–106. Journal of International Affairs Editorial Board.
36. Secret Intelligence Service MI6 (2021). Richard Moore First Public Speech: Human Intelligence in the Digital Age. *Secret Intelligence Service MI6*.
37. House of Commons Defence Committee (2018). Rash or Rational? North Korea and the threat it poses.
38. Baronchelli, A. (2018). Conflict in Cyber-Space: The Network of Cyber Incidents, 2000–2014. *Peace Economics, Peace Science and Public Policy*, Vol 24, De Gruyter.
39. UK Government (2022). National Cyber Force. *gov.uk*.
40. NCA (2019). Cyber crime. *National Crime Agency*.
41. Danish Defence Intelligence Service (DDIS) (2016). *The DDIS Intelligence Risk Assessment 2016*. DDIS.
42. CPNI (2021). Espionage. *Centre for the Protection of National Infrastructure*.
43. Verizon (2021). Verizon 2020-2021 Cyber-Espionage Report. Verizon.
44. Detica *et al.* (2011). The Cost of Cyber Crime.
45. MI5 (2022). Joint address by MI5 and FBI Heads.
46. FBI (2022). Director's Remarks to Business Leaders in London. *Federal Bureau of Investigation*.
47. NCSC *et al.* (2020). Advisory: APT29 targets COVID-19 vaccine development. NCSC.
48. Gillis, A. What is a Supply Chain Attack? *SearchSecurity*.
49. New Zealand's National Cyber Security Centre (2021). Supply Chain Cyber Security. New Zealand's National Cyber Security Centre.
50. Bendiek, A. *et al.* (2021). Attribution: a major challenge for EU cyber sanctions: an analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW. *SWP Research Paper*, Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs.
51. Fournier, J. (2020). What Is a Managed Service Provider (MSP)? *HCM Works*.
52. DCMS (2022). Proposal for legislation to improve the UK's cyber resilience. UK Government.
53. CrowdStrike (2021). What is a Supply Chain Attack? *Crowdstrike*.
54. MITRE (2022). Supply Chain Compromise. *MITRE ATT&CK*.
55. PwC UK *et al.* (2017). *Operation Cloud Hopper*.
56. Herr, T. *et al.* (2020). Breaking trust: Shades of crisis across an insecure software supply chain. Atlantic Council.
57. Office of the Director of National Intelligence (2022). Annual Threat Assessment of the U.S. Intelligence Community. Office of the Director of National Intelligence.
58. Slowick, J. (2019). CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. Dragos Inc.
59. Smith, M. (2022). Russia has been at war with Ukraine for years – in cyberspace. *The Conversation*.
60. CISA (2018). Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. United States Cybersecurity and Infrastructure Security Agency.
61. Jensen, B. *et al.* (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, Vol 42, 212–234. Routledge.

62. Karlsen, G. H. (2019). Divide and rule: ten lessons about Russian political influence activities in Europe. *Palgrave Commun*, Vol 5, 1–14. Palgrave.
63. Commission on the Theft of American Intellectual Property (2017). IP Comission Report Update. The National Bureau of Asian Research.
64. Barlett, J. (2020). Exposing the Financial Footprints of North Korea's Hackers. *Centre for a New American Security*.
65. Caesar, E. (2021). The Incredible Rise of North Korea's Hacking Army. *The New Yorker*.
66. Nichols, M. (2019). North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report. *Reuters*.
67. GCHQ (2018). Director's speech at Cyber UK 2018.
68. Finkle, J. *et al.* (2016). Bangladesh Bank heist similar to Sony hack; second bank hit by malware. *Reuters*.
69. General Intelligence and Security Service (GISS) (2018). *General Intelligence and Security Service (GISS) Annual Report 2017*.
70. Joint Committee on the National Security Strategy (2018). Cyber Security of the UK's Critical National Infrastructure.
71. NCSC (2019). NCSC CAF guidance. 5.
72. NCSC (2018). New Cyber Attack categorisation system to improve UK response to incidents. *NCSC*.
73. Psaki, J. (2022). Press Briefing by Press Secretary Jen Psaki, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and Deputy National Security Advisor for International Economics and Deputy NEC Director Daleep Singh, February 18, 2022. *The White House*.
74. NCSC (2018). Annual Review 2018.
75. Buchanan1, B. *et al.* (2020). Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis. *Texas National Security Review*, Vol 3, 54–81.
76. Department of Homeland Security, Office of Intelligence and Analysis (2022). Warning of Potential for Cyber Attacks Targeting the United States in the Event of a Russian Invasion of Ukraine. Department of Homeland Security, Office of Intelligence and Analysis.
77. Fischerkeller, M. P. *et al.* (2017). Deterrence is Not a Credible Strategy for Cyberspace. *Orbis*, Vol 61, 381–393.
78. Kuhne, S. (2019). The Importance of Modernizing Legacy Systems. *Gavant Software*.
79. Cabinet Office The Digital, Data and Technology Playbook.
80. McKinsey & Company (2020). Digital supply chain planning and execution. *McKinsey & Company Operations*.
81. Cyberspace Solarium Commission (2020). Building a Trusted ICT Supply Chain. Cyberspace Solarium Commission.
82. DCMS Cyber Security Breaches Survey 2022.
83. Burton, S. D. *et al.* (2021). The UK Code of Practice for Consumer IoT Cybersecurity: where we are and what next. Geopolitics of Industrial Internet of Things Standards (GISt) and Building Evidence for CoP Legislation (BECL).
84. Hakmeh, J. *et al.* (2022). What is a cyber attack? *Chatham House*.
85. Pamment, J. *et al.* (2019). Hybrid Threats: 2007 Cyber Attacks on Estonia. NATO Strategic Communications Centre of Excellence.
86. Knapp, E. D. *et al.* (2015). Chapter 7 - Hacking Industrial Control Systems. in *Industrial Network Security (Second Edition)*. (eds. Knapp, E. D. et al.) 171–207. Syngress.
87. Sanger, D. E. (2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*.
88. Collins, S. *et al.* (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*, Vol 7, 80–91. Routledge.
89. Alvarez, J. (2015). Stuxnet: The world's first cyber weapon. *Center for International Security and Cooperation, Freeman Spogli Institute for International Studies*.
90. Křoustek, J. (2017). WannaCry ransomware that infected Telefonica and NHS hospitals is spreading aggressively, with over 50,000 attacks so far today. *Avast*.
91. UK Government (2017). Foreign Office Minister condemns North Korean actor for WannaCry attacks. *gov.uk*.
92. Ghafur, S. *et al.* (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digit. Med.*, Vol 2, 1–7. Nature Publishing Group.
93. Department of Health (2018). Investigation: WannaCry cyber attack and the NHS. National Audit Office.
94. NCSC A guide to ransomware.
95. Ivanov, A. *et al.* (2017). ExPetr/Petya/NotPetya is a Wiper, Not Ransomware. *Kasperspy Securelist*.
96. The Council of the European Union (2020). COUNCIL IMPLEMENTING REGULATION (EU) 2020/1125. European Union.
97. United States District Court Western District Of Pennsylvania (2020). *United States Of America V. Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevichfrolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, Petr Nikola Yevich Pliskin*. United States District Court Western District Of Pennsylvania.
98. Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*.
99. Mandia, K. (2020). Global Intrusion Campaign Leverages Software Supply Chain Compromise. *FireEye*.
100. UK Government (2021). Russia: UK exposes Russian involvement in SolarWinds cyber compromise. *gov.uk*.
101. Council of the EU (2021). China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory. *European Council*.
102. Corera, G. (2021). China accused of cyber-attack on Microsoft Exchange servers. *BBC News*.
103. UK Government (2018). UK and allies reveal global scale of Chinese cyber campaign. *gov.uk*.
104. The White House (2021). The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China. *The White House*.
105. Guerrero-Saade, J. A. *et al.* (2022). AcidRain | A Modem Wiper Rains Down on Europe. *SentinelOne*.
106. Viasat (2022). KA-SAT Network cyber attack overview.
107. Suess, J. (2022). Jamming and Cyber Attacks: How Space is Being Targeted in Ukraine. *RUSI*.
108. UK Government (2022). Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion. *gov.uk*.
109. Wilson, R. (2019). Information Warfare: Fabrication, Distortion and Disinformation: A Case Study and Anticipatory Ethical Analysis. in *Proceedings of the 18th European Conference on Cyber Warfare and Security (ECCWS)*. 596–603.
110. Lukito, J. (2020). Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017. *Political Communication*, Vol 37, 238–255.
111. DCMS (2021). Online Media Literacy Strategy.
112. Ingram, H. J. (2020). The Strategic Logic of State and Non-State Malign 'Influence Activities': Polarising Populations, Exploiting the Democratic Recession. *The RUSI Journal*, Vol 165, 12–24.
113. House of Commons Digital, Culture, Media and Sport Committee (2019). *Disinformation and 'fake news': Final Report*.
114. Christie, L. (2021). COVID-19 vaccine misinformation.

115. Lella, I. *et al.* (2021). Threat Landscape for Supply Chain Attacks. ENISA.
116. Waseem, Z. *et al.* (2021). Scams and Misinformation Challenges. *Stay Safe Online, National Cybersecurity Alliance*.
117. IISS (2021). Cyber Capabilities and National Power: A Net Assessment. IISS.
118. Gold, J. (2020). The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'. 30. CCDCOE.
119. Brooke-Holland, L. (2022). What is NATO? House of Commons Library.
120. Mattis, J. N. (2018). Transcript of News Conference by Secretary Mattis at NATO Headquarters, Brussels, Belgium. *U.S. Department of Defense*.
121. NATO (2022). Cyber defence.
122. NATO (2021). Resilience and Article 3. *NATO*.
123. NATO (2020). NATO Cyber Defence.
124. Libicki, M. *et al.* (2021). Cyberspace Escalation: Ladders or Lattices? 60–72.
125. Stoltenberg, J. (2019). Nato will defend itself. *Prospect Magazine*.
126. Hollis, D. (2021). A Brief Primer on International Law and Cyberspace. *Carnegie Endowment for International Peace*.
127. Mačák, K. (2021). Unblurring the lines: military cyber operations and international law. *Journal of Cyber Policy*, Vol 6, 411–428. Routledge.
128. Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and Insights. Social Science Research Network.
129. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2021). Tallinn Manual 3.0 Call for Contributions.
130. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
131. Lewis, J. (2022). Creating Accountability for Global Cyber Norms. CSIS.
132. Kostyuk, N. *et al.* (2018). Determinants of the Cyber Escalation Ladder. *The Cyber Defense Review*, Vol 3, 123–134. Army Cyber Institute.
133. Valeriano, B. *et al.* (2018). How We Stopped Worrying about Cyber Doom and Started Collecting Data. *Politics and Governance*, Vol 6, 49–60.
134. Soesanto, S. *et al.* (2021). Chapter 20: Cyber Deterrence: The Past, Present and Future. in *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century - Insights from Theory and Practice*. (eds. Osinga, F. et al.) Springer-Verlag Berlin Heidelberg.
135. Nye, Jr., J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, Vol 41, 44–71.
136. Thornton, R. *et al.* (2019). Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom. *Journal of Cyber Policy*, Vol 4, 257–274. Routledge.
137. Tran Dai, C. *et al.* (2018). Challenges and opportunities for cyber norms in ASEAN. *Journal of Cyber Policy*, Vol 3, 217–235. Routledge.
138. Kulikova, A. (2021). Cyber norms: technical extensions and technological challenges. *Journal of Cyber Policy*, Vol 6, 340–359. Routledge.
139. Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber attacks. *Journal of Cybersecurity*, Vol 7, tyab009.
140. Kello, L. (2021). Cyber legalism: why it fails and what to do about it. *Journal of Cybersecurity*, Vol 7, tyab014.
141. Wintour, P. (2018). UK accuses Kremlin of ordering series of 'reckless' cyber-attacks. *The Guardian*.
142. Paulus, A. (2022). Why Germany should practice the cyber norms it preaches. *Heinrich-Böll-Stiftung*.
143. UN Office for Disarmament Affairs Open-ended Working Group. *un.org*.
144. OSCE (2022). Cyber/ICT Security. *osce.org*.
145. Organization for Security and Co-operation in Europe (2016). Permanent Council Decision No. 1202. *osce.org*.
146. European Telecommunications Standards Institute *etsi.org*.
147. Simonelis, A. (2005). A Concise Guide to the Major Internet Bodies. *Uniquity*.
148. Carnegie Endowment for International Peace Cyber Norms Index and Timeline. *carnegieendowment.org*.
149. Hurel, L. M. *et al.* (2018). Unpacking cyber norms: private companies as norm entrepreneurs. *Journal of Cyber Policy*, Vol 3, 61–76. Routledge.
150. Farrand, B. *et al.* (2018). Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism. in *Security Privatization: How Non-Security-Related Private Businesses Shape Security Governance*. 197–217.
151. Cybersecurity Tech Accord. *cybertechaccord.org*.
152. Meyer, P. (2018). Global Cyber Security Norms: A Proliferation Problem? ICT for Peace Foundation.
153. Global Commission on the Stability of Cyberspace (2019). Advancing Cyberstability.
154. LRIRE (2020). The Law & Politics of Cyberattack Attribution. *UCLA Law Review*.
155. Zabierek, L. *et al.* (2021). Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure. Belfer Center for Science and International Affairs.
156. UK Government (2022). UK government assess Russian involvement in DDoS attacks on Ukraine.
157. Egloff, F. J. *et al.* (2021). Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*, Vol 0, 1–32. Routledge.
158. Cyberspace Solarium Commission (2020). Cyberspace Solarium Commission Strategy. Cyberspace Solarium Commission.
159. Keitner, C. I. (2019). Attribution by Indictment. *American Journal of International Law*, Vol 113, 207–212. Cambridge University Press.
160. Egloff, F. (2020). Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy*, Vol 41, 55–81.
161. Rid, T. *et al.* (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, Vol 38, 4–37.
162. Cavelty, M. D. *et al.* (2022). Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation. Routledge.
163. The United States Department of Justice (2019). Former U.S. Counterintelligence Agent Charged With Espionage on Behalf of Iran; Four Iranians Charged With a Cyber Campaign Targeting Her Former Colleagues.
164. The United States Department of Justice (2022). Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide.
165. CISA (2022). Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector. *United States Cybersecurity and Infrastructure Security Agency*.
166. BBC News (2015). Sony cyber-attack: North Korea faces new US sanctions. *BBC News*.
167. Council of the EU (2019). Cyber-attacks: Council is now able to impose sanctions. *European Council*.
168. Taddeo, M. (2018). The Limits of Deterrence Theory in Cyberspace. *Philos. Technol.*, Vol 31, 339–355.
169. Helwig, N. *et al.* (2020). Sharpening EU sanctions policy for a geopolitical era. Finnish Institute of International Affairs.
170. van der Meer, S. (2017). Deterrence of Cyber-Attacks in International Relations: denial, retaliation and signaling.

Netherlands Institute of International Relations 'Clingendael'.
171. Schulze, M. (2019). Cyber Deterrence is Overrated. Stiftung Wissenschaft und Politik.
172. Smeets, M. *et al.* (2018). Offensive cyber capabilities: To what ends? in *2018 10th International Conference on Cyber Conflict (CyCon)*. 385–400.
173. Blair, R. *et al.* IT Resilience - 7 Tips for Improving Reliability, Tolerability and Disaster Strategy. Gartner.
174. ITU (2022). Global Cybersecurity Index 2020. Geneva, Switzerland.
175. Home Office (2021). Proscribed terrorist groups or organisations. *gov.uk*.
176. (2020). The ethics of offensive cyber operations. *The Foreign Policy Centre*.
177. Welburn, J. W. *et al.* (2019). Cyber Deterrence or: How We Learned to Stop Worrying and Love the Signal. RAND Corporation.
178. DCMS (2022). 2022 Cyber security incentives and regulation review.
179. About Internet Society. *internetsociety.org*.
180. Our Mission: Enabling a Secure and Trustworthy Internet - Global Cyber Alliance. *globalcyberalliance.org*.
181. UKRI Academic centres of excellence in cybersecurity research. *www.ukri.org*.
182. DCMS (2021). Regulating consumer smart product cyber security - government response.
183. Hutton, G. *et al.* (2022). The Product Security and Telecommunications Infrastructure Bill 2021-22. House of Commons Library.
184. House of Commons (2022). National Security Bill. *UK Parliament*.
185. Dawson, J. (2021). Counter state threats legislation. House of Commons Library.
186. EDRI (2017). Proposed Espionage Act threatens free speech in the UK. *European Digital Rights (EDRi)*.
187. DCMS *et al.* (2022). Press release: Online safety law to be strengthened to stamp out illegal content. *gov.uk*.
188. Joint Committee on the Draft Online Safety Bill (2022). Draft Online Safety Bill. *UK Parliament*.
189. Department for Business, Energy & Industrial Strategy (2022). National Security and Investment Act: guidance on notifiable acquisitions. *gov.uk*.
190. NCSC (2017). Cyber Essentials: Overview. *National Cyber Security Centre*.
191. NCSC (2022). We think Cyber Essentials is, well, still essential ... *NCSC*.
192. Department for Business (2021). Business population estimates for the UK and regions 2021: statistical release. *gov.uk*.
193. NCSC (2021). Active Cyber Defence Introduction. *NCSC*.
194. NCSC (2022). Active Cyber Defence Services.
195. NCSC (2022). CNI Hub.
196. Klimburg, A. *et al.* (2018). A Balance of Power in Cyberspace. Hague Centre for Strategic Studies.
197. Smith, B. (2018). An important step toward peace and security in the digital world. *Microsoft On the Issues*.
198. Mee, P. *et al.* (2021). Cybersecurity is too big for governments or firms to handle alone. *World Economic Forum*.
199. Rosenbach, E. *et al.* (2019). Governing Cyberspace: State Control vs. The Multistakeholder Model. *Belfer Center for Science and International Affairs*.
200. Joint Committee on the National Security Strategy *Cyber Security Skills and the UK's Critical National Infrastructure*.
201. DCMS (2020). Cyber security incentives & regulation review: government response to the call for evidence.
202. DCMS (2020). *Post-Implementation Review of the Network and Information Systems Regulations 2018*.
203. UK Government (2022). New laws proposed to strengthen the UK's resilience from cyber attack. *gov.uk*.
204. Dawson, J. *et al.* (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, Vol 9,
205. Mennecozzi, G. M. *et al.* (2021). Bridging the Gap: Adapting a Security Education Platform to a New Audience. in *2021 IEEE Global Engineering Education Conference (EDUCON)*. 153–159.
206. Zatterin, G. *et al.* Cyber security skills in the UK labour market 2022. DCMS, Ipsos.
207. DCMS (2020). Cyber security skills in the UK labour market 2020.
208. McHenry, D. *et al.* (2021). *Cyber security skills in the UK labour market 2021: findings report*. 84. DCMS, Ipsos Mori.
209. DCMS (2022). Embedding standards and pathways across the cyber profession by 2025. *gov.uk*.
210. Geneva Dialogue on Responsible Behaviour in Cyberspace (2020). Security of digital products and services: Reducing vulnerabilities and secure design: Good practices'. Geneva Dialogue on Responsible Behaviour in Cyberspace.
211. Scarfone, K. *et al.* (2009). Cyber Security Standards. in *Wiley Handbook of Science and Technology for Homeland Security*. 1–10. John Wiley & Sons, Ltd.
212. Eurasia Group (2018). The Geopolitics of 5G. Eurasia Group.
213. Strumpf, D. (2019). Where China Dominates in 5G Technology. *Wall Street Journal*.
214. Feldstein, S. (2019). The Global Expansion of AI Surveillance.

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Amber Keegan for researching this briefing, to the Institution of Chemical Engineers and the Materials Processing Institute for funding her Ashok Kumar Fellowship, and to all contributors and reviewers. For further information on this subject, please contact the co-author, Dr Lydia Harriss.