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.

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

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.

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.2,9
- 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.

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.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.24,73,74 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 infrastructure7 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.96,80 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).

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; or to erode trust, for example in authorities or democracy. The EU Agency for Cybersecurity (ENISA) says that there was a rapid rise in disinformation operations during the COVID-19 pandemic. ENISA highlight social media as a key way of spreading disinformation, although it is also spread in other ways, such as by email (POSTnote 559).

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. 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. 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. NATO facilitates information sharing and assistance between allies to prevent, mitigate and recover from cyber-attacks. The UK has offered its offensive cyber capabilities (see page 4) in support of agreed NATO goals. 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.

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

Accepted norms may help the international community to hold accountable those who operate outside “acceptable” behaviour, and inform decisions about proportionate responses. However, there is debate about their efficacy. The UK participates in various state-led groups that aim to establish norms, including the UN Open-Ended Working Group, the Organisation for Security and Co-operation in Europe, and standards bodies such as the European Telecommunications Standards Institute.

Box 3: Examples of suspected state-backed attacks

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Attribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bronze Soldier (2007)</td>
<td>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.</td>
</tr>
<tr>
<td>Stuxnet (2010)</td>
<td>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.</td>
</tr>
<tr>
<td>WannaCry (2017)</td>
<td>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 appointments. Ransomware typically renders files inaccessible by encryption and demands a ransom to restore them.</td>
</tr>
<tr>
<td>NotPetya (2017)</td>
<td>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.</td>
</tr>
<tr>
<td>SolarWinds (2020)</td>
<td>Cyber intrusion operation carried out via a supply chain compromise of IT management software from SolarWinds. Impact on the UK was low, but 18,000 organisations were affected globally. Attributed to Russia.</td>
</tr>
<tr>
<td>Microsoft Exchange (2021)</td>
<td>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. Attributed to China.</td>
</tr>
<tr>
<td>ViaSat (2022)</td>
<td>A DDoS attack on global satellite communications company, ViaSat, on the day Russia invaded Ukraine. ViaSat said that this affected several thousand customers in Ukraine and tens of thousands of others across Europe. Attributed to Russia.</td>
</tr>
</tbody>
</table>

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. Motivations for public attributions include apprehending attackers (if possible), deterring future attacks, and highlighting unacceptable behaviours to reinforce norms. States typically offer few details with attributions. 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. States are sometimes sanctioned for cyber operations, such as the EU’s sanctions against Russia in 2019 after the NotPetya attack. The UK Government says that attribution is a critical part of deterring cyber threats. However, some analysts question the efficacy of deterrence, including through attributions and sanctions.

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.
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).\(^5\),\(^6\) 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.\(^67\),\(^75\) 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].)\(^10\),\(^184\)-\(^186\)
  - **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 implementcore 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 pathways, 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\(^44\) 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

3. Computer Security Resource Center  Glossary - Cyberspace. NIST.
40. Danish Defence Intelligence Service (DDIS) (2016). _The DDIS Intelligence Risk Assessment 2016._ DDIS.
44. MIS (2022). _Joint address by MIS and FBI Heads._
46. NCSC et al. (2020). _Advisory: APT29 targets COVID-19 vaccine development._ NCSC.
47. Gillis, A. _What is a Supply Chain Attack?_ SearchSecurity.
53. MITRE (2022). _Supply Chain Compromise_. MITRE ATT&CK.
58. Smith, M. (2022). _Russia has been at war with Ukraine for years – in cyberspace_. The Conversation.


71. NCSC (2019). NCSC CAF guidance. S.

72. NCSC (2018). New Cyber Attack categorisation system to improve UK response to incidents. NCSC.


79. Cabinet Office. The Digital, Data and Technology Playbook.


82. DCMS Cyber Security Breaches Survey 2022.


90. Kroustek, J. (2017). WannaCry ransomware that infected Telefónica and NHS hospitals is spreading aggressively, with over 50,000 attacks so far today. Avast.


94. NCSC. {\textit{A guide to ransomware}}.


115. Lella, I. et al. (2021). Threat Landscape for Supply Chain Attacks. ENISA.
117. IISS (2021). Cyber Capabilities and National Power: A Net Assessment. IISS.
122. NATO (2021). Resilience and Article 3. NATO.
123. NATO (2020). NATO Cyber Defence.
146. European Telecommunications Standards Institute etsi.org.
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.
Netherlands Institute of International Relations

‘Clingendael’.


176. (2020). The ethics of offensive cyber operations. The Foreign Policy Centre.


187. DCMS et al. (2022). Press release: Online safety law to be strengthened to stamp out illegal content. gov.uk.


191. NCSC (2022). We think Cyber Essentials is, well, still essential. NCSC.


193. NCSC (2021). Active Cyber Defence Introduction. NCSC.


203. UK Government (2022). New laws proposed to strengthen the UK’s resilience from cyber attack. gov.uk.


