

2. United Kingdom

The United Kingdom is a highly capable cyber state, with clear strategic oversight at the political level. It has world-class strengths in its cyber-security ecosystem, centred on the National Cyber Security Centre, and in its related cyber-intelligence capability centred on the Government Communications Headquarters. There is a strengthening partnership between government and industry, and an attempt to develop a whole-of-society approach to improve national cyber-security capability. There is significant investment in cyber research and development and innovation, with the government looking to the strengths of the private sector and academia. To increase its reservoir of cyber skills, the UK appears to be pursuing widespread and innovative collaboration across all sectors. Its economy, society and armed forces all greatly benefit from digital connectivity but are potentially more vulnerable as a result. Perhaps the

UK's key weaknesses, in common with most other states, are shortfalls in its skilled cyber workforce and that it cannot afford to invest in cyber capabilities on the same scale as the United States or China. These are offset in part by the breadth and depth of the UK's proven international alliances, particularly with the US. Another area of potential comparative weakness is that the UK lacks the indigenous industrial base required to build and export the equipment that might ultimately dictate the future of global cyberspace, meaning it can only seek to manage the attendant risks. The country uses its international influence to shape the future of cyberspace and is a strong advocate for the application of existing international law to the use of cyber capabilities. The UK has developed, and used, offensive cyber capabilities since at least the early 2000s, and is investing further in their expansion.

Strategy and doctrine

Cyber defence has been highlighted as a high-priority national-security issue in the United Kingdom's strategy papers since the late 1990s, and featured prominently in the UK's first National Security Strategy in 2008. The first National Cyber Security Strategy (NCSS) was produced in 2009 and updated in 2011 and 2016. Although they concentrated on cyber security and

defence, those strategies also included clear allusions to the development of offensive capabilities.

The 2016 NCSS lays out a strategy of 'defend, deter and develop', with the last of those three rubrics covering the national cyber-industrial capability, the skills base and the country's associated analytical capability.¹ One indication of the importance the UK places on cyber

List of acronyms

DCMS Department for Digital, Culture, Media & Sport
GCHQ Government Communications Headquarters
ICT information and communications technology
JFCyG Joint Forces Cyber Group
MoD Ministry of Defence
NAO National Audit Office

NCF National Cyber Force
NCSC National Cyber Security Centre
NCSP National Cyber Security Programme
NCSS National Cyber Security Strategy
NOCP National Offensive Cyber Programme

issues is the sizeable and increasing investment the government made in cyber capabilities during a period of financial austerity: the 2016–21 plan saw a doubling of investment to £1.9 billion (US\$2.5bn). The increase was justified by asserting that previous commitments had ‘not achieved the scale and pace of change required to stay ahead of the fast-moving threat’.²

The NCSS is supported by a National Cyber Security Programme (NCSP) and, for offensive cyber, a National Cyber Force (NCF). The NCF was publicly avowed in December 2020 and subsumed the previously existing National Offensive Cyber Programme (NOCP), which had been running since 2014. Together, the NCSP and the new NCF execute the national cyber strategy under the oversight of government ministers and parliamentary committees.³

The NCSP is strongly geared to improving public- and private-sector cooperation on cyber security under the leadership of the UK’s innovative National Cyber Security Centre (NCSC). Delivery of the NCSP is evaluated annually by the UK’s National Audit Office (NAO) and the results made public.

Now continued under the NCF, the NOCP’s role was described as providing a ‘dedicated capability to act in cyberspace’ with ‘appropriate offensive cyber capabilities that can be deployed at a time and place of our choosing, for both deterrence and operational purposes, in accordance with national and international law’.⁴ The UK first avowed its offensive cyber capability in 2015, stating a preparedness to use cyber capabilities to deter and counter threats, including for warfighting. A 2019 speech by the UK’s Chief of the Defence Staff highlighted the UK’s perception of the daily ‘war’ in cyberspace resulting from great-power competition and the battle of ideas with non-state actors, while noting that this was not war as it had been understood in the past.⁵

Guided by national strategies and investment, the armed forces set their strategy and capability objectives through directives from the secretary of state for defence and the Chief of the Defence Staff. The need for and use of cyber capabilities is copiously covered in UK military doctrine, with the Ministry of Defence (MoD) Joint Doctrine Publication 0-50 on ‘UK Cyber Doctrine’ presumably the most important (its contents remain classified).⁶ In general, publicly available UK doctrine

points to the perceived need to integrate the military’s approach to cyber, electromagnetic, information and kinetic operations,⁷ and gives a view of military cyber operations not dissimilar to the US concept of information dominance, but without using the term.

Governance, command and control

Strategic direction on cyber capability is set by the prime minister and other key cabinet members, supported by officials in the Cabinet Office, and enacted through the NCSS, NCSC and NCF. Ministerial roles are well established, with the home secretary, defence secretary, foreign secretary and secretary of state for Digital, Culture, Media and Sport (DCMS) all having defined strategic roles. The supporting civilian cyber-security ecosystem is described later in this chapter.

Unlike the US and some other states, the UK has not created a military cyber command with unified command and control of all military (but in the US case, only military) cyber operations and assets, both defensive and offensive. That said, the UK military is fully responsible for protecting its own networks. Command and control for doing so rests with UK Strategic Command, enacted through its subordinate Joint Forces Cyber Group (JFCyG). Created in 2013 and originally known as the Defence Cyber Operations Group, the JFCyG commands the centre for UK military cyber security (MoD Corsham), various joint-forces cyber units, tri-service information-assurance units and a cyber-reserve component based on assets in the British Army, Royal Air Force and Royal Navy. But it is in command and control of offensive cyber that the UK is most unlike the US, having developed a globally unique solution with the creation of the NCF.

The NCF combines the relevant cyber elements of Government Communications Headquarters (GCHQ) – the UK’s cyber-intelligence and security agency – with those of the MoD, the Secret Intelligence Service (SIS) and the Defence Science and Technology Laboratory in a single organisation under unified command. It covers the full range of the UK’s national-security priorities, from tackling serious criminality, international terrorism and the malign activity of states to preparing for war. As such, there is nothing comparable anywhere else in the world. In US terms, it is the equivalent of

bringing together the offensive cyber capabilities of Cyber Command, the National Security Agency, Central Intelligence Agency and Federal Bureau of Investigation into a single organisation. The NCF commander reports to both the head of GCHQ and the commander of Strategic Command, with NCF operations politically authorised by either the foreign secretary or the defence secretary, depending on the nature of the mission. While predominantly focused in peacetime on tackling non-military targets, the NCF also prepares the UK for the use of cyber capabilities in armed conflict.

Greater efficiency is one reason why the UK has chosen to create the NCF, having fewer personnel and less money to devote to cyber than, for example, the US or China. It gives the UK greater operational agility, allowing it to prioritise across all national requirements, concentrating skills and technical capabilities where they are needed most. It is a move that also recognises the need to ensure that military operations in cyberspace take full account of the domain's centrality to civilian society and the global economy, allowing for full civilian–military operational coordination.

Core cyber-intelligence capability

In the last 30 years, GCHQ has successfully adapted the UK's century-old signals-intelligence and information-security capability so that it can obtain the breadth of intelligence needed from cyberspace. The evidence for this is the UK's history of detecting, attributing and disrupting malign cyber activity, its intelligence-led disruption of terrorist activity, its efforts against online criminality, and the many hints in the Edward Snowden leaks about the sophistication and global reach of GCHQ's capabilities. It is safe to assume, drawing on material from the Snowden leaks, that the UK has retained a world-leading cryptographic capability, continuing a tradition of mathematical ingenuity that dates back to Alan Turing and beyond. GCHQ's capabilities are amplified by its long-standing and close partnership with the US and by its membership of the Five Eyes intelligence alliance. In common with the other

Five Eyes nations, the UK has, with GCHQ, centred its core cyber-security and cyber-intelligence capabilities in a single organisation, drawing on the traditional intelligence and security principle that poachers make the best gamekeepers and vice versa. The NCSC is an integral part of GCHQ.

The evidence also points to a mature system for assessing, sharing and making use of cyber intelligence, including an ability to fuse it with other sources of information. This is founded on the UK's long-established Joint Intelligence Committee and the maturity of its wider intelligence system. Reports by parliamentary committees indicate close collaboration between GCHQ and the other two main intelligence agencies – SIS, specialising in overseas human intelligence collection and covert operations, and MI5, specialising in the UK's domestic security. For specifically cyber-security-related intelligence, the NCSC acts as a hub for combining high-grade secret intelligence with information acquired by the private sector.

The UK's armed forces both benefit directly from the above capabilities and have their own cyber-intelligence assets that add to the UK's overall situational awareness. These include 'field' interception undertaken by each armed service and by special forces, intelligence assessment undertaken by the MoD's Defence Intelligence organisation, and the ability to fuse cyber information quickly with intelligence from other military assets.

Cyber empowerment and dependence

The UK is one of the most digitally connected European countries, with a very high internet penetration rate (above 90%). According to the approach adopted by the G20, the UK's digital economy ranked second in the world in its share of GDP (just over 55%) in 2018, with the US in first place (59%) and Japan (46%) in third.⁸ While this reliance on digital capacity and digital enterprise brings significant economic and social benefits to the UK, the government has nevertheless noted the vulnerability inherent in such dependence. It is therefore working with the private sector to gauge more accurately the extent of UK network resilience now and

The UK has retained a world-leading cryptographic capability

in the future, including the degree to which the digital economy is dependent on the commercial energy network. One stated aim, stemming from the 2019–20 debate about the use of Huawei equipment, is to create a greater diversity of ICT suppliers and solutions to serve UK needs.

The UK armed forces are a microcosm of the wider situation. Their activities are greatly enabled by a sophisticated networked capability, with the ability to communicate, move and fuse data globally for tasks such as targeting, navigation, surveillance, and command and control. They are heavily reliant on space-based technology for most of this capability.⁹ The MoD is consequently moving towards the idea of ‘defence as a platform’, which includes smaller contracts and shorter development time frames, potentially as a way of reducing its reliance on a small number of large IT systems with long development time frames.

The UK’s approach to research and development (R&D) and innovation in cyber capabilities and related technology, such as artificial intelligence (AI), is highly distributed across the public and private sectors and academia, in part mirroring the cyber-security ecosystem described below. The stated aim is to recognise where industry can innovate more quickly than government, and therefore to foster strong public–private partnership wherever possible. The result is a plethora of cyber-specific incubators, accelerators, start-ups, research institutes and academic centres of excellence. The amount of investment across such a distributed system is difficult to ascertain, but some UK cyber-security companies are now valued in the hundreds of millions of pounds, with a presumed commensurate investment in R&D. Large companies from the US defence sector, such as Lockheed Martin and Northrop Grumman, are also investing heavily in UK cyber R&D.

It is evident that the AI sector in the UK has great strengths. By 2018, AI-related companies numbered about 6,000, of which about 2,800 advertised themselves as working in that field.¹⁰ Of those, about 400 specialised in deep learning (using automated data analytics), with another 300 focusing on robotics, virtual reality and the Internet of Things. About 250 firms

were working on recognition technologies and another 250 on data-mining for business solutions. UK universities are ranked among the most influential business and academic organisations in the world in AI research: for example, in 2020, in a top-40 list based on contributions to the two leading academic conferences in the field, Oxford was in seventh position, Cambridge in 22nd and University College London in 30th.¹¹ China’s Tsinghua University was in ninth position, Peking University in 24th and Shanghai Jiaotong University in 43rd. By this measure the UK is approximately at level pegging with China, at least for now. However, in a separate ranking of countries according to their contributions to AI research in the health sector, based simply on the number of titles published in the previous 40 years, the UK did not figure in the top 20.¹² This illustrates that in a field as wide and diverse as AI, a state can lead in one area of research and be weak in another.

The UK government states that ‘having a sustainable supply of home-grown cyber security professionals is part of our wider ambition to be a world leader in cyber security. Put simply, we cannot be a global leader in cyber security without access to the best cyber security talent.’¹³ A 2020 government inquiry, however, found that the UK lacked cyber expertise across the board, from

The AI sector in the UK has great strengths

basic skills to specialists.¹⁴ In response to those findings, a wide range of measures have been introduced, largely driven by the NCSC and DCMS, with the aim of stimulating growth in the requisite skills through the education sector and wider society. The CyberFirst initiative launched in May 2016, for example, has been expanded and is now part of an £84 million (US\$114m) government cyber-education programme. It has courses for school-age children, undergraduate bursaries, degree apprenticeships, and sponsored doctorates in cyber security and related fields. There is significant emphasis on encouraging girls to develop cyber-security skills. It is too soon to assess the success of these initiatives, but the diagnosis of the problem appears to be accurate and the proposed treatment potentially effective.

The UK’s armed forces are again a microcosm of the broader UK picture. The MoD works on cyber R&D with a range of companies including BAE Systems, Lockheed

Martin, Northrop Grumman, QinetiQ, Raytheon, Roke and Thales UK. There are cyber-recruitment initiatives across each armed service, and for a Joint Cyber Reserve Force. However, specialists with deep experience of the UK's cyber capabilities assert that its armed forces will find it hard to develop the required depth of expertise if they do not emulate the US by creating opportunities for entire military careers in cyber. It is believed that the UK military is addressing this under the new NCF construct.

Perhaps the greatest area of complexity for the UK, however, is the limited degree to which it controls its own national telecommunications infrastructure, and whether this really matters. Design of the network is currently undertaken by the company BT, which used to have a monopoly as the UK's sole network provider. Due to its size, BT runs what might be considered the core public network, though providers such as Virgin Media compete with it, especially since the migration of the network to new-generation IP-based services. BT is the dominant provider of telephone exchanges and owns much of the access-network infrastructure (the element 'downstream' of the exchanges). But all the telecoms companies present in the UK (including those with foreign ownership) have their own networks, while the UK is looking to open up as much of BT's network and infrastructure to other firms as possible. In reality, it is impractical for competing operators to replicate completely the scale of BT's network, so instead they rely on acquiring capacity or facilities from it. The result is that those companies can install their own hardware, voice lines and broadband services and can take over the existing physical lines. Overall, the growth and development of the UK's telecommunications network has been driven principally by market forces.

UK mobile networks include foreign-owned equipment that uses either networks provided by the foreign companies or BT's 'backbone' networks. For the UK's 4G mobile networks, for example, the Chinese company Huawei provides radio equipment, such as masts, that broadcast mobile-network signals and relay communications back to the core network for several

operators. Huawei's contribution ranges from 5% of the equipment used by O2 to more than 30% of that used by Vodafone. Huawei's involvement (right down to the coding) is closely monitored by the UK government at a facility in the town of Banbury. Other foreign suppliers used across the network include Cisco, Ericsson, Fujitsu, Nokia and Siena, with no equivalent oversight. In short, the UK relies to a considerable extent on foreign manufacture of much of the equipment underpinning its telecommunications, from microchips to communications switches. This infrastructure complexity is typical of the Western model of a free, multi-stakeholder internet.

Data crossing the UK network takes the most suitable route across various platforms and systems, based on factors such as cost, time and available bandwidth. Much of the data is encrypted by 'over the top' applications such as Facebook, Google, Microsoft, Signal, Telegram and WhatsApp, making the content largely invisible to the infrastructure providers (of whatever nationality), and to the UK government, unless they receive assistance from the providers of those applications.

The complexity of its networks is in many ways an advantage for the UK since it provides a certain level of redundancy and resilience. For example, the country is so well connected to the internet through autonomous nodes (second only to Germany in that respect) that multiple nodes would have to be put out of action for there to be a significant impact on the functioning of the system. Also, the UK has 88 undersea-cable landing points in its territory, providing a high degree of redundancy if several of the cables were disabled, although the risk that even one of the cables might be interfered with or cut by an adversary remains a concern. It is still the case that the UK's networks rely on foreign supply chains to a greater extent than those of the US or China and are therefore more exposed to the attendant risk. Furthermore, the UK's weaker position in the global market for network infrastructure compared with the US or China means it has less influence than they do in shaping the physical infrastructure of global

The UK's networks rely on foreign supply chains to a greater extent than those of the US or China

cyberspace.¹⁵ The government seems to have recognised the risk to its national networks, having announced initiatives to improve security standards for equipment and to encourage greater diversification of suppliers.

In July 2020 the government ended a long-running controversy when it announced a ban on purchases of Huawei equipment for its new 5G networks, to come into force in 2021, and the stripping out of all Huawei equipment from all its networks by 2027.¹⁶ This overturned an earlier government decision to manage the security risk by limiting the presence of Huawei equipment to non-sensitive parts of the networks. However, an intervening US ban on the export of US microchip technology to Huawei undermined the quality and reliability of the Chinese company's product, forcing the UK's hand. The pressure applied by the US to both Huawei and the UK therefore seemed to be more about curtailing the global expansion of Chinese digital technology than dealing with an immediate security risk.

Cyber security and resilience

The UK has developed a national cyber-security ecosystem that aspires to a whole-of-society approach, seeking to ensure that government, the private sector, academia and individual citizens work together to improve overall national cyber security. The efficacy of that ecosystem was reflected in the UK being ranked first out of 175 countries in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union.¹⁷

At the heart of the ecosystem sits the NCSC, which became operational in October 2016. This rationalised the government's cyber-security effort, bringing together functions previously distributed across several departments and aiming to provide a central point of reference on cyber security for ministers and the private and public sectors.¹⁸ The NCSC includes the UK's national Computer Emergency Response Team (CERT-UK).

As part of GCHQ, the NCSC is able to draw upon the government's principal source of cyber expertise and threat data. The NCSC's headquarters was deliberately kept separate from GCHQ, however, so it would be more accessible to private companies, the media and the public. The NCSC has good connections with UK law enforcement, where cyber-security capabilities have been developed by the National Crime Agency's

National Cyber Crime Unit and by the Regional Organised Crime Units. Through GCHQ, the NCSC is also organisationally connected to the NCF.

There has been a strengthening partnership between government and the private sector on cyber security. Through its Cyber Security Information Sharing Partnership the NCSC has designed a way for government and industry to exchange information in real time, and it has accredited about 100 companies as suppliers of cyber security to government through its Cyber Growth Partnership. The UK's critical national infrastructure officially consists of 13 sectors,¹⁹ each of which is required by government to produce an annual Sector Security and Resilience Plan, incorporating cyber-security issues, while individual companies are responsible for their own business-continuity and resilience plans. There is a proven system for incident-alerting and response, cyber-defence exercises involving government and industry, and a dedicated national risk register. Awareness programmes for the wider public include Cyber Aware, Cybersecurity Challenge, Cyber Essentials and Get Safe Online.

Importantly, there was evidence of a shift in approach in the 2016 version of the UK's cyber-security strategy. The pre-2016 versions of the strategy had relied on market forces to bring about more secure practices among companies but had not achieved the scale and pace of change required to keep ahead of threats. In the 2016 strategy the government adopted a more interventionist role to deliver the required improvements. This was partly embodied in the NCSC's Active Cyber Defence initiative, also launched in 2016, which has involved working with internet service providers to find ways of blocking and disrupting malicious activity at the network level, with the aim of protecting most UK citizens from most high-volume/low-sophistication attacks most of the time. The first tranche of activity has focused on citizens' interactions with government and has had an impact on, for example, the phishing threat – the UK's share of global phishing attacks fell from 5.3% to 2.2% between 2016 and 2018, according to the NAO.²⁰ The plan is now to incorporate UK industry sectors within this approach.

While the various processes that make up the UK's cyber-security ecosystem appear to be well established, it is harder to evaluate the human and technical capacity that supports it. The investment of £1.9bn

(US\$2.5bn) under the current five-year programme is substantial in the context of overall UK government funding, although the NAO has reported some delivery issues. The 740 staff allocated to the NCSC also represent a substantial commitment but are only a small part of the personnel dedicated to cyber security across government and the private sector. The approximately 100 companies accredited to deliver cyber-security services to government indicate considerable private-sector capacity,²¹ with a 2020 report noting a 44% increase in the number of cyber-security firms in the UK, and a 37% increase in cyber-related jobs, between 2017 and 2019.²² The challenge for the UK may lie in ensuring it has sufficient personnel with crucial deep cyber-security skills and expertise, hence the various upskilling initiatives being driven by the NCSC.

The current state of cyber security in the UK is reflected in a 2020 report²³ showing that cyber attacks are being detected more frequently, with almost half of businesses reporting cyber-security breaches during the previous 12 months. However, businesses also reported a higher level of resilience, and the average cost of individual breaches was quite low (£3,230, or less than US\$5,000). The qualitative research nevertheless revealed some confusion about incident reporting and highlighted the important role for key players such as banks and insurance companies in guiding the private sector on cyber security.

Global leadership in cyberspace affairs

The UK aspires to shape the global cyber future by pursuing international action and exerting its influence in international forums. It advocates the application of existing international law (including the laws of armed conflict) in cyberspace and promotes the establishment of voluntary, non-binding norms of state behaviour and the development and implementation of confidence-building measures.

The UK has sponsored or led cyber-security initiatives in the United Nations, the European Union and the Commonwealth. For example, it has implemented international programmes helping more than 80 countries to improve their cyber security, supported by the UK-developed 'Cybersecurity Capacity Maturity Model for Nations';²⁴ and in May 2019, alongside the

Netherlands, the UK drove through the adoption of an EU sanctions regime to directly penalise computer hackers. The UK's withdrawal from the EU may weaken important channels for influence over pan-European cyber-security policy and cyber-crime control. The UK has actively participated in the UN Group of Governmental Experts on cyberspace security since its creation in 2004.²⁵

The UK has long-standing international alliances on cyber intelligence and cyber security, for example with its Five Eyes partners, a broad range of European states and as a member of NATO. There is evidence of growing cooperation on cyber security with a wider range of countries across the Middle East, the Asia-Pacific and Latin America. There is also evidence of the UK operating with close allies on offensive cyber operations, for example with the US and Australia against the Islamic State (also known as ISIS or ISIL). The UK and the US signed an agreement in 2016 to advance their collaborative development of both offensive and defensive cyber capabilities. The UK's cyber capability is almost certainly amplified by this proven ability to work in concert with other cyber-capable nations.

Offensive cyber capability

Government ministers have stated unambiguously that the UK is prepared to use cyber capabilities to deter and counter threats, including from terrorists, serious criminals and malign cyber actors; that they consider offensive cyber operations integral to modern warfare; and that the UK military is committed to using its offensive cyber capability as a warfighting tool.²⁶ Offensive cyber is covered in detail in published UK military doctrine, including its use to create freedom of manoeuvre, to project power, for destructive military effect and for deterrence.

The UK's development of an offensive cyber capability has been a joint venture between GCHQ and the MoD. From 2014, this was under the auspices of the NOCP, which was subsumed in 2020 by the NCF. It seems the investment of people and money was already substantial under the NOCP and will increase under the NCF. Evidence from parliamentary committees in 2016–17 shows that the NOCP had instigated a step change in the UK's effort on offensive cyber, with the development of the full spectrum of capabilities from those required

for peacetime influence-and-information operations to those relevant to high- and low-intensity combat. The committees also highlighted an increase in GCHQ efforts on computer-network exploitation (hacking), which is a vital part of an effective offensive cyber capability.

The evidence available on actual capability is understandably scant, given the need for secrecy, although in 2018 the UK became one of only three countries to have publicly acknowledged the use of offensive cyber capabilities (the others being the US and Australia). Judging from indications in the Snowden leaks, GCHQ had been pioneering the development and use of offensive cyber techniques since the turn of the millennium, particularly for disruptive cognitive effect against international terrorists.²⁷ Furthermore, as well as exercising its capabilities on cyber ranges and incorporating cyber dimensions into war games, it is clear that the UK has used its military operations in Afghanistan and elsewhere as operational proving grounds for its integration of cyber action into modern warfare.²⁸

Whether for intelligence-gathering or offensive purposes, the UK states that it will use its cyber capabilities responsibly and according to strict thresholds dictated by domestic and international law. The overarching principle in UK law is that all such operations have to be proved necessary and proportionate, and that

if they are for military effect, they must also proceed through the MoD's well-established and ministerially led targeting process (adding the principles of discrimination and humanity). This means considerations of unintended consequences and collateral damage are an integral part of the UK system. Like the US, though, the UK reserves the right to use its offensive cyber capabilities for more than deterrent effect, its strategy stating that it will deploy them at a time and place of its choosing, including for national operational purposes.²⁹ Like other cyber-capable states that operate within strict international and domestic legal limits, the UK probably needs to find a way of generating a better-informed public debate on the use of offensive cyber to ensure it retains the necessary political licence to operate. This will probably entail a greater level of openness on its plans for developing and using such capabilities.

Perhaps the principal challenge facing the UK's offensive cyber capability is the need for continued investment both in terms of money and personnel, especially in order to increase capacity in core technical skills. This is something the creation of the NCF is intended to address. Overall, however, the available evidence seems to back the UK claim in its 2016 NCSS that, together with the US, it is a world leader on offensive cyber.

Notes

- 1 HM Government, 'National Cyber Security Strategy 2016–2021', 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
- 2 *Ibid.*, p. 9.
- 3 'The National Security Secretariat, a division of the Cabinet Office (the Department), manages the Programme on the National Security Adviser's behalf.' See National Audit Office, 'Progress of the 2016–2021 National Cyber Security Programme', 15 March 2019, p. 20, <https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf>.
- 4 HM Government, 'National Cyber Security Strategy 2016–2021', p. 51.
- 5 Dominic Nicholls, 'Britain is "at war every day" due to constant cyber attacks, Chief of the Defence Staff says', *Telegraph*, 29 September 2019, <https://www.telegraph.co.uk/news/2019/09/29/britain-war-every-day-due-constant-cyber-attacks-chief-defence>.
- 6 A public source giving some insight into doctrine is UK Ministry of Defence, 'Joint Doctrine Note 1/18, Cyber and electromagnetic activities', 21 February 2018, <https://www.gov.uk/government/publications/cyber-and-electromagnetic-activities-jdn-118>.
- 7 UK Ministry of Defence, 'Joint Concept Note 2/17, Future of Command and Control', September 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643245/concepts_uk_future_c2_jcn_2_17.pdf.

- 8 Longmei Zhang and Sally Chen, 'China's Digital Economy: Opportunities and risks', International Monetary Fund Working Paper, no. WP/19/16, 17 January 2019, p. 4, <https://www.imf.org/en/Publications/WP/Issues/2019/01/17/Chinas-Digital-Economy-Opportunities-and-Risks-46459>.
- 9 As well as access to US systems, the UK military has its own Skynet satellite constellation. The MoD is considering options for maintaining the continuity of Skynet services beyond August 2022, when the current Skynet 5 financing arrangement comes to an end.
- 10 Organisation for Economic Co-operation and Development, 'Measuring the Digital Transformation: A roadmap for the future', 11 March 2019, p. 34, <https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm>.
- 11 Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, <https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-states-stay-ahead-of-china-61cf14b1216>. This ranking has weaknesses, however, as do all rudimentary scoring systems.
- 12 Bach Xuan Tran et al., 'Global evolution of research in artificial intelligence in health and medicine: A bibliometric study', *Journal of Clinical Medicine*, vol. 8, no. 3, 14 March 2019, p. 9, <https://www.mdpi.com/2077-0383/8/3/360/pdf>.
- 13 Department for Digital, Culture, Media and Sport, 'Initial National Cyber Security Skills Strategy: Increasing the UK's cyber security capability – a call for views', 3 May 2019, <https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views>.
- 14 Daniel Pedley et al., 'Cyber security skills in the UK labour market 2020: Findings report', 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/869506/Cyber_security_skills_report_in_the_UK_labour_market_2020.pdf.
- 15 The UK is nonetheless an active exporter of telecommunications equipment. For example, BT and Vodafone install and operate systems in many other countries. In any case, it could be argued that the nationality of the design of a completed product is not a reliable guide to where that product's components were manufactured – hence the impact on US chip manufacturers of the US ban on Huawei products. Supply-chain risks may be an inevitable consequence of the globalisation of the development and production of technology. If so, all states will need to manage those risks, and the UK's approach may later be regarded as having been in the vanguard.
- 16 UK Government, 'Huawei to be removed from UK 5G networks by 2027', 14 July 2020, <https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027#:~:text=HUAWEI%20will%20be%20completely%20removed,sanctions%20against%20the%20telecommunications%20vendor>.
- 17 International Telecommunication Union, 'Global Cybersecurity Index 2018', pp. 30, 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
- 18 Those functions include the production of national assessments, the protection of critical national infrastructure, information assurance, and national-level computer-emergency response teams.
- 19 The 13 sectors making up the UK's critical national infrastructure are chemicals, civil nuclear, communications, defence, emergency services, energy, finance, food, government, health, space, transport and water – see Centre for the Protection of National Infrastructure, 'Critical National Infrastructure', <https://www.cpni.gov.uk/critical-national-infrastructure-o>.
- 20 National Audit Office, 'Progress of the 2016–2021 National Cyber Security Programme', 2019, p. 11, <https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf>.
- 21 More UK companies offer cyber-security services than the 100 or so that are accredited – the UK government estimates the number is around 800. On one level, such diversity is a strength; on another, it dilutes their market presence compared with large, well-known foreign companies such as FireEye. The UK's cyber-security industry has many start-ups and small companies struggling to grow; some market consolidation is needed.
- 22 Sam Donaldson et al., 'UK Cyber Security Sectoral Analysis 2020', Department for Digital, Culture, Media and Sport, January 2020, pp. 2, 44, 63, 73, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/861945/UK_Cyber_Sectoral_Analysis_2020_Report.pdf.
- 23 UK Department for Digital, Culture, Media and Sport, 'Cyber Security Breaches Survey 2020', 26 March 2020, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020>.
- 24 Global Cyber Security Capacity Centre, 'Cybersecurity Capacity Maturity Model for Nations', Oxford University, 2017, <https://cybilportal.org/tools/cybersecurity-capacity-maturity-model-for-nations-cmm-revised-edition>.
- 25 Since a UN General Assembly resolution in 2004, a UN Group of Governmental Experts (GGE) has convened for two-year

terms to address international-security aspects of cyberspace. It was known as the GGE on 'Developments in the Field of Information and Telecommunications in the Context of International Security' until 2018, when it was renamed the GGE on 'Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. In cyberspace-policy circles it is common to refer to it simply as 'the GGE'. See UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', <https://www.un.org/disarmament/ict-security>.

26 For a collection of such statements, see GCHQ, 'National Cyber Force transforms country's cyber capabilities to protect the UK', November 2020, <https://www.gchq.gov.uk/news/national-cyber-force#:~:text=Defence%20Secretary%20Ben%20>

Wallace%20said,ability%20to%20conduct%20cyber%20operations.

27 The UK government continues to neither confirm nor deny the information leaked by Snowden.

28 Apart from its statements with regard to the Islamic State, the UK has made no formal acknowledgement of its offensive cyber operations. But for a mention of such operations in Afghanistan, see Gordon Corera, 'UK's National Cyber Force comes out of the shadows', BBC News, 20 November 2020, <https://www.bbc.com/news/technology-55007946>.

29 UK Parliament, 'Electronic Warfare: Question for Ministry of Defence', UIN 201591, tabled on 12 December 2018, <https://questions-statements.parliament.uk/written-questions/detail/2018-12-12/201591>.