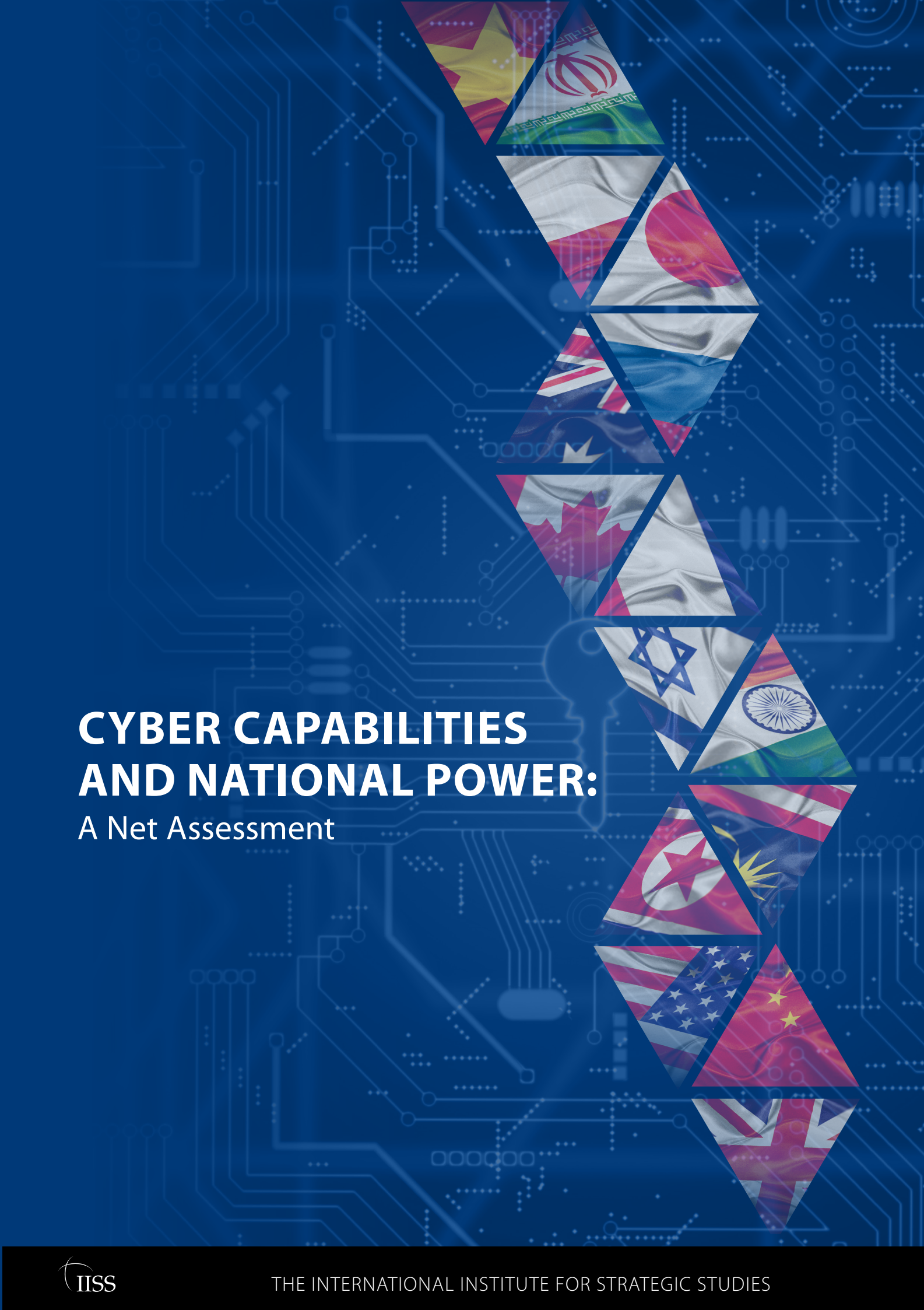

CYBER CAPABILITIES AND NATIONAL POWER:

A Net Assessment

IISS

THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES

CYBER CAPABILITIES AND NATIONAL POWER:
A Net Assessment

Contents

Preface

In February 2019 the International Institute for Strategic Studies (IISS) announced in a *Survival* article its intention to develop a methodology for assessing the cyber capabilities of states and how they contribute to national power.[1] Here, we set out that methodology, use it to assess 15 countries, and draw out the overarching themes and conclusions.

This report is intended to assist national decision-making, for example by indicating the cyber capabilities that make the greatest difference to national power. Such information can help governments and major corporations when calculating strategic risk and deciding on strategic investment.

While other organisations have developed index-based methodologies,[2] with most focusing principally on cyber security, our methodology is broader: it is principally qualitative and analyses the wider cyber ecosystem for each country, including how it intersects with international security, economic competition and military affairs.

The 15 studies represent a snapshot in time: the national circumstances of each state will of course evolve, and cyber strategies and investments will face challenges from many sources, including the COVID-19 pandemic. Nevertheless, for each state, most policies and trends in capability are likely to endure.

The studies have been conducted against the background of intensifying international confrontation in cyberspace. Several reference points can be cited by way of illustration. In 2015, China's new military strategy declared that 'outer space and cyber space have become new commanding heights of strategic competition' between states.[3] In 2016, the Unites States accused the Russian government, and President Vladimir Putin personally, of ordering a sustained information attack on the US presidential election.[4] In May 2019, then-president Donald Trump foreshadowed a technology war with China if it continued its malign actions in cyberspace.[5] In March 2020, Trump declared a national emergency in cyberspace,[6] the fourth time in five years that a US president had done so. In April 2021, China referred to the US as the 'champion' of cyber attacks.[7] A month later, the G7 foreign ministers' meeting called on both Russia and China to bring their cyber activities into line with international norms.[8] Overall, this report provides substantial further evidence that, for many countries, cyber policies and capabilities have moved to centre stage in international security.

The countries covered in this report are the US, the United Kingdom, Canada and Australia (four of the Five Eyes intelligence allies); France and Israel (the two most cyber-capable partners of the Five Eyes states); Japan (also an ally of the Five Eyes states, but less capable in the security dimensions of cyberspace, despite its formidable economic power); China, Russia, Iran and North Korea (the principal states posing a cyber threat to Western interests); and India, Indonesia, Malaysia and Vietnam (four countries at earlier stages in their cyber-power development).

We assess each country's capabilities in seven categories:

- Strategy and doctrine
- Governance, command and control
- Core cyber-intelligence capability
- Cyber empowerment and dependence
- Cyber security and resilience
- Global leadership in cyberspace affairs
- Offensive cyber capability

Key assessments are summarised in a single paragraph at the start of each chapter.

The IISS intends to continue its research into cyber power and to lead expert dialogue on the subject, guided

by its teams in Berlin, London, Manama, Singapore and Washington DC. In future publications we intend to conduct a deeper analysis of offensive cyber campaigns.

We have relied on the input of many experts and wish to thank all of them. The IISS is the sole author of this publication and takes full responsibility for its contents.

Notes

1 See Marcus Willett, 'Assessing Cyber Power', *Survival: Global Politics and Strategy*, vol. 61, no. 1, February–March 2019, pp. 85–90.

2 Examples include the International Telecommunication Union's Global Cybersecurity Index, the Potomac Institute's Cyber Readiness Index 2.0 and the Harvard Kennedy School's National Cyber Power Index 2020.

3 State Council Information Office of the People's Republic of China, 'China's Military Strategy', 27 May 2015, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

4 United States Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, 6 January 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

5 White House, 'Executive Order on Securing the Information and Communications Technology and Services Supply Chain', 15 May 2019, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain.

6 White House, 'Text of a Letter from the President to the Speaker of the House of Representatives and the President of the Senate', 30 March 2020, https://trumpwhitehouse.archives.gov/briefings-statements/text-letter-president-speaker-house-representatives-president-senate-67.

7 Nick Wadhams, 'U.S.–China Talks in Alaska Quickly Descend Into Bickering', Bloomberg, 19 March 2021, https://www.bloomberg.com/news/articles/2021-03-18/u-s-china-meeting-will-underscore-biden-s-continuity-with-trump.

8 'G7 Foreign and Development Ministers' Meeting, May 2021: Communiqué', London, 5 May 2021, http://www.g7.utoronto.ca/foreign/210505-foreign-and-development-communique.html.

The Cyber-Power Project: Context and Methodology

Over the last 20 years, cyber capabilities have become a formidable new instrument of national power. As well as using such capabilities to obtain state secrets from each other, as in traditional espionage, states have also used them for a range of other, more threatening purposes. These include bolstering their own economic development by stealing intellectual property; threatening to disrupt the financial institutions, oil industries, nuclear plants, power grids and communications infrastructure of states they regard as adversaries; attempting to interfere in democratic processes; degrading and disrupting military capabilities in wartime; and, in one case, constraining the ability of another state to develop nuclear weapons.

The state-on-state cyber operations revealed in the media include those by the United States and Iran against each other; Israel and Iran against each other; Russia against Estonia, Georgia and Ukraine; and Chinese attempts to steal intellectual property on an industrial scale. Russian operations against the democratic process in the US and United Kingdom have received considerable attention, as have the US retaliatory operations against the St Petersburg-based group deemed to be partly responsible. A Russian cyber operation against the US in late 2020, the 'SolarWinds hack', has also been prominent. There have been operations by Iran against Saudi Arabia, by North Korea against Sony Pictures and the global banking system, and by the US, the UK and Australia against the Islamic State (also known as ISIS or ISIL). Some operations have been conducted in an unrestrained manner, resulting in many unintended victims. For example, the NotPetya malware that the Russians used against Ukraine severely damaged the Maersk shipping line, and the WannaCry malware the North Koreans used against the global banking system affected the UK's National Health Service.

These media reports only tell a small part of the story. State cyber operations to reconnoitre and gain a presence on relevant networks are occurring every second and are now a permanent feature of cyberspace. The risk of miscalculation is high. Reconnaissance or prepositioning could be misinterpreted by the defender as an actual attack, and therefore provoke retaliation. Inserted code could malfunction, causing an accident. Escalation could easily spiral out of control as a result, which is perhaps the gravest risk entailed in state-on-state cyber operations. Other risks include the acquisition of state capabilities by criminals or terrorists, and the ease with which states can find highly effective offensive tools on the open market (the so-called 'low point of entry').

In short, cyberspace has become, perhaps inevitably, a key and risky new environment for statecraft and competition between states in the twenty-first century. It has also become a major, and arguably *the* major, domain for organised crime. There are no reliable estimates of the costs of cyber crime at a national level.[1] It is possible to document lower-end estimates of certain types of cyber crime, such as credit-card fraud,[2] but such sub-categories cannot capture the full range of economic costs from the many types of cyber crime that extend beyond direct losses, for example by causing reputational damage or degradation of share value. Since 2017 there has been a surge in reported losses from ransomware (malware that prevents access to critical data until the required ransom amount is paid), which have totalled tens of billions of dollars. The damage done by the various types of cyber crime has inevitably led to a new world of litigation, regulatory fines and insurance claims. In addition, terrorist groups such as ISIS and al-Qaeda aspire to become more cyber-capable, while political-activist groups of all stripes now view

cyberspace as an indispensable medium through which to advance their causes. The threats to any state and its citizens in cyberspace are many and varied.

States are therefore trying to mitigate the risks that cyber threats pose to their digital economies, critical national infrastructure and citizens by making considerable investment in protective cyber-security capabilities. These are fuelling the growth of a globalised cyber-industrial sector. States are incorporating cyber capabilities into their national investment strategies and their military doctrines and plans, and increasing the tempo of their cyber-related activities.

More fundamentally, states have realised the degree to which their economic prosperity, as well as their national security and geostrategic influence, is dependent on their management of cyber risks. This becomes even more critical as the everyday lives of their businesses and citizens become more internet-dependent, given the roll-out of the Internet of Things ('smart' homes in smart cities, with driverless vehicles on smart roads). States are therefore trying to shape, influence and, in some cases, control the future design and governance of the internet. Some states, led by Russia and China, have for many years been advocating in the United Nations for a new internet-governance model that would see greater state control rather than the predominant 'multi-stakeholder' balance between governments, the private sector, interest groups and individuals, commonly referred to as 'internet freedom'. At the heart of the national strategies of the US and China, and the trade war between them, is competition for control over the technologies that physically underpin the future of cyberspace – such as microchip production, computer assembly, mobile internet (such as 5G), cloud architectures, cables and routers. In 2020, moves by the US to ban the Chinese software applications TikTok and WeChat under the Clean Network programme[3] added a further dimension, in some ways paralleling China's long-standing ban on US software applications as part of its 'Great Firewall'. Given the geostrategic, economic and security advantages that a leadership position in advanced information technologies would bring, states in the twenty-first century recognise they can only be superpowers if they are digital superpowers.

The huge surge in the number of people working digitally from home as a result of COVID-19 has had obvious implications for cyber security, with a spike in malign cyber activity. This should not be a surprise, as the restrictions on human mobility have massively decreased the opportunities for criminality and state espionage in the physical world while increasing them commensurately in the digital one. Opportunities are now proliferating for individuals who can steal, defraud and spy digitally from home. However, there are perhaps other, more positive lessons to draw. Before COVID-19, the world was already dealing with another kind of virus pandemic – in cyberspace. Every day, national security and global prosperity are being significantly damaged by cyber infections. While of course the threat to human health and life is less serious than that from biological viruses, it nevertheless remains conceivable that cyber operations, if unchecked, will cause even greater destruction, and potentially also deaths, either by accident or design. Lessons from the way states have collaborated to fight COVID-19 – for example on movement restrictions and the supply of personal-protection equipment, and in seeking to develop therapeutic remedies and viable vaccines – might therefore be applicable to dealing with this cyber pandemic. For example, the international approach to establishing meaningful norms of behaviour for cyberspace could be intensified. States could increase their efforts to work together to combat cyber crime globally, perhaps with some form of sharing between states of the technical 'DNA' of cyber-criminal threats in the same way that the DNA of COVID-19 has been shared. Moreover, some of the post-COVID-19 lessons about the importance of increasing national and global resilience to strategic shocks will be equally applicable to plans for dealing with a cyber catastrophe.

As national prosperity, security and statecraft have become increasingly reliant on cyberspace, understanding the development and use of cyber power by states has become paramount. That is why the IISS has developed a methodology for assessing national cyber power.

Methodology

A number of organisations have developed methodologies for measuring cyber power. The majority have focused principally on cyber security and have been index-based. By contrast, the IISS methodology is

holistic, covering all the facets outlined above, and is principally qualitative.

This report does not consider non-state actors unless we assess that the development and/or use of their cyber capabilities is directed by a state. We include the Iranian Cyber Army, for example, as part of Iran's state capability, and the St Petersburg-based Internet Research Agency as part of Russia's. As for cyber criminality, it is beyond our scope apart from in cases where there is a proven nexus with a state.

We assess each country in seven categories:

- Strategy and doctrine
- Governance, command and control
- Core cyber-intelligence capability
- Cyber empowerment and dependence
- Cyber security and resilience
- Global leadership in cyberspace affairs
- Offensive cyber capability

Under **strategy and doctrine**, we analyse the most important government documents, regardless of the formal titles assigned to them. We review, for example, documents that set out priorities and budgets, describe management policy or organisational change, or aim to raise public awareness of national strategy. Unlike most index-based models, we examine the evolution and judge the quality of the strategies and doctrines, rather than just noting their existence.

Under **governance, command and control**, we cover the top-level governmental and military structures, as well as those at the more operational level. We show how these structures have evolved over time, as well as examining their effectiveness today.

At the heart of any nation's cyber capability, both defensive and offensive, is the ability to identify and understand threats and opportunities in cyberspace. Many sources of information contribute to such situational awareness, but the most vital is a **core cyber-intelligence capability** (also commonly referred to as a 'cyber-espionage' capability). While we have included this as a category, it has proven hard to measure objectively given the understandable lack of publicly available information.

In considering **cyber empowerment and dependence**, we are addressing a frequently asked question: can a state best protect itself against a cyber-capable adversary by isolating from the global internet? Our assumption is that any dependence on internet connectivity brings with it an inherent vulnerability; but it also brings the data, global reach and networking that empower twenty-first-century economies, statecraft and warfare. We therefore consider both sides of the coin. To understand the contours of the dependence, we look at the vibrancy and scale of the country's digital economy, including its international relationships in this area. We are guided by the G20's definition of the digital economy, adopted in 2016, which sees it as the entirety of the economic impacts of modern information and communications technology (ICT) throughout all sectors, rather than just the estimated value of ICT companies' output of goods and services. We also look at what may be termed sovereign economic power in the cyber domain. It is beyond the scope of this report to analyse the whole scientific and technological foundation of each country's digital economy; instead we use assessments of research into and use of artificial intelligence (AI) as a proxy indicator.[4]

The category of **cyber security and resilience** covers a state's core cyber-security capability, including its ability to respond to, and recover from, significant cyber incidents and emergencies. It also includes the setting of security standards, technical innovation, sector-specific risk management, the effectiveness of the indigenous cyber-security industry, and the degree to which the country has been able to develop and expand a cyber-specialist workforce. To provide something of a standardised measure of national cyber security, we include in each study a reference to the country's ranking in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union (ITU).

Under **global leadership in cyberspace affairs**, we consider the extent to which a country engages in, influences and attempts to lead international collaboration on cyber matters. The category therefore includes relevant international diplomacy, formal alliances, engagement in international forums, and participation in international technical cooperation and arrangements for mutual assistance.

Our use of the term **offensive cyber** covers cyber operations that are principally intended to deliver an effect

rather than those principally intended to gather intelligence. Such operations range from those designed for cognitive effects to those designed for physical destruction – whether in peace or war, and regardless of whether the operations are run by civilians or the military, or whether the targets are civilian or military. Various other terms are commonly used for such operations, including 'computer-network attack', 'computer-network operations', 'cyber-enabled information operations and warfare', 'cyber-influence operations' and 'cyber effects'. Terms such as 'cyber espionage' and 'computer-network exploitation' apply to intelligence-gathering and are covered in this report under core cyber-intelligence capability. We also consider the factors that dictate each country's use of its offensive cyber capability, including political will, legal regimes and ethical frameworks.

The countries assessed in this report are:

- Four of the five states that make up the Five Eyes intelligence alliance: the US, the UK, Canada and Australia
- Three close cyber allies of the Five Eyes partners: France, Israel and Japan
- The four states commonly viewed as the principal cyber threats to the Five Eyes and allied states: China, Russia, Iran and North Korea
- Four developing cyber states: India, Indonesia, Malaysia and Vietnam.[5]

There are of course many cyber-capable states absent from this list – notably Germany and some of the Nordic and Baltic states in Europe; New Zealand; Singapore and South Korea in the Far East; and Saudi Arabia and some other Gulf states in the Middle East. Taiwan is also worthy of close analysis. This report includes no North or sub-Saharan African states, and none in Central or South America. With this first compilation, our intention was to apply the methodology to most of the significant current cyber powers and to a small selection of developing powers, before applying it to a wider range of states in due course.

Each study was undertaken by a specialist, answering a set of detailed questions for each of the seven categories in the methodology. The resulting narratives inevitably reflect the specific circumstances and worldview of each country, as well as large divergences in the quality and quantity of available source material. The content of the studies has been harmonised only to the extent needed to address the main research questions.

The data underpinning our analysis was gathered through research of published material and, in some cases, interviews with experts. The amount of publicly available data on cyber capabilities is greater than might be expected, making feasible some objective measurement. This is particularly true of the essential protective domain and any national economic and industrial components. The key facts in the studies include those that have emerged from published strategies and plans, known investment of financial and human resources, known operational use, and testing and exercising activities. We have also taken account of various non-governmental and academic indices, including the ITU's Global Cybersecurity Index. Offensive cyber and intelligence capabilities are, unsurprisingly, the most difficult to measure objectively. For example, an absence of evidence for their existence does not equate to evidence of their absence. Qualitative judgement therefore also forms a key part of the 15 country studies.

Analysis

This section sets out some of the key themes to emerge from our analysis of the 15 countries, along with observations about their relative standing in terms of cyber power.

The challenges of national strategy for cyberspace

All the countries assessed in this report, even the most powerful, have struggled to shape durable policy frameworks for cyberspace, either for the purpose of exploiting new opportunities or defending against new threats. The dynamism of the cyber environment (in technologies, economics, politics and security affairs) has forced leading countries to undertake reappraisals and revisions to key strategy documents on an almost continuous basis. In ways that vary from country to country, the traditional structures of government, corporate management and social organisation consistently struggle to adapt in a timely fashion. Though

'disruptive' is perhaps an overused term, it is the predominant characteristic of the forces at play.

Our research confirms that all countries are still in the early stages of coming to terms with the strategic implications of cyberspace. Ambitions and imaginative visions are plentiful and have already been manifested in pioneering projects that include smart cities, driverless cars, remote surgery and military robotics. In most countries, however, matching those ambitions to national decision-making processes has proved difficult. The consumer-driven private sector remains well ahead of government regulation and policy. In several countries, the cyber-industrial complex is racing ahead with surveillance and intelligence capabilities, prompting dire warnings about the direction in which human society may be headed. Some governments now see cyberspace as an arena of existential competition, even as they try to put in place international collaborative systems to dampen competitive impulses. A sense of crisis and inadequacy is pervasive in political circles, with private actors seemingly saying 'catch me if you can' to governments as they race to maximise immense profits. The impacts on the formulation of national strategy have been both positive and negative, but few governments believe their current strategies are likely to achieve their stated goals.

The inter-state competition in cyberspace has become a contest over the ability to develop effective strategies for national development and then implement them. Few countries have scored highly in this regard, but the smaller countries, such as Israel, seem to have performed better than the larger ones.

The role of intelligence agencies

Secrecy is one of the issues that impedes a more informed international approach to managing the risks entailed in cyber operations, as sensitive intelligence capabilities and the agencies that run them are at the heart of both the defensive and offensive operations of all the leading states. For example, capabilities designed by Five Eyes countries to detect online terrorist activity after 9/11 have also proved essential in detecting and attributing cyber attacks. Likewise, sensitive hacking techniques that states have developed in order to collect intelligence on adversaries provide most of what is needed for an offensive cyber operation. As a result, organisations such as the National Security Agency in the US and Government Communications Headquarters in the UK have been the driving forces behind the national approach to cyber in their respective countries.

The US and the UK are among the countries where the need for greater transparency on cyber security has been recognised. There have been various initiatives to improve openness, including a greater sharing of data on threats and vulnerabilities with industry and the public. On offensive cyber, it has so far proved difficult even to find the language for a more informed national and international public debate, but such an effort remains essential if the risks are to be properly managed.

High-tech industrial competition

The future cyber resilience of every state depends on the physical infrastructure underpinning the global internet, how it is built and by whom. Given the heated debate in 2020 about Huawei, and the presumed risks entailed in using foreign equipment in critical national infrastructure, it is instructive to examine the current state of play when it comes to national representation in global digital assets. The nationalities of the 51 telecommunications or technology companies that appear in the 2020 *Fortune* 'Global 500' rankings reveal the extent to which those two sectors remain dominated by the US and its allies or close partners,[6] which together provide no fewer than 43 of the companies: 16 are American; ten are Japanese; six Taiwanese; two South Korean; eight Western European; and one Mexican. The remaining eight companies are Chinese, with their market share expanding in East and Southeast Asia, sub-Saharan Africa and Latin America as part of China's Digital Silk Road programme.

For all countries, the use of digital technology relies to some extent on foreign-produced components, with the Chinese situation particularly instructive. China describes the eight American companies whose products are prevalent in its digital infrastructure as the 'eight guardian warriors': Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle and Qualcomm. One way China has sought to mitigate this perceived vulnerability is to involve US companies in its internal cyber-security governance, including for national technical standards,

allowing it some oversight of the use of US technology in its networks. But achieving such oversight is difficult, given the extent to which some US and Chinese entities are entangled in cyberspace. For example, in September 2019, IBM and the Bank of China announced that they would expand their existing relationship to co-create new digital innovations for the financial industry, supporting tens of trillions of dollars of daily global financial exchanges across shared infrastructure with agreed common or compatible standards. Whether the technical competition between the US and China, which intensified in 2020, will inevitably lead to an untangling of such technical solutions, or even whether such an untangling is possible in today's interconnected global economy, remains to be seen.

Whole-of-society approach to cyber security

The most cyber-capable states are all pushing for what could be described as a 'whole of society' response to cyber security. This entails close partnership and sharing of information between the public and private sectors and academia, and similarly close civilian–military partnerships. It also includes innovative upskilling and education schemes, and campaigns aimed at heightening public awareness.

There are differences of approach, however. Predictably, the more authoritarian regimes are employing a top-down method, with strict governmental control and direction, and are arguably more focused on controlling the spread of content (ideas) over the internet than on technical protection of critical networks. Accordingly, China, Iran and Russia are each attempting to develop their own 'sovereign' state-controlled internets to enable them to isolate, if necessary, from a global internet that they perceive as dominated by the US.

Liberal democracies, on the other hand, tend towards a more distributed approach, with national innovation largely driven by the private sector and academia, and with a key concern being how the privacy of individual citizens' data is protected. The result is a vibrant, multibillion-dollar cyber-security industry, as well as large investments in state-of-the art security by the internet service providers themselves. These states also strive to retain a global, multi-stakeholder internet, with governance balanced across national governments, the private sector, non-governmental organisations and academia.

It is notable that in the ITU's Global Cybersecurity Index, the leading liberal democracies tend to score considerably higher on cyber security than the authoritarian states. This in part reflects the greater vibrancy of their cyber-security industrial sectors. In the US, this sector contributes a much larger portion of national GDP than, for example, in China, although the gap has begun to narrow slightly.

In short, both methods for creating a whole-of-society approach to cyber security seem to have strengths and weaknesses, but the one employed by liberal democracies may be the more effective overall.

Offensive cyber

The leading cyber powers employ a variety of approaches to the development and use of offensive cyber capability. Those that can afford the largest investments in terms of personnel and money, such as the US and China, tend to maintain a clear separation between military- and civilian-owned capabilities, even where military–civilian cooperation is strong. Some other countries, such as Australia, France, Israel and the UK, tend towards a more fused military–civilian approach, compensating for a lack of resources through arguably greater operational agility.

What sets the US apart on offensive cyber is its ability to employ a sophisticated, surgical capability at scale

Most states keep the development and use of offensive cyber capability under strict government control and within the bounds of a strict legal regime. However, some governments – Russia and Iran in particular – are more tolerant of 'patriotic hackers' (private hackers who further the interests of the state) and cyber-criminal groups operating from their territories, sometimes even coordinating with them.

There are also some key doctrinal differences. For both China and Russia, what the West calls 'offensive cyber' is just the technical component of a wider information-operations capability. It is just one means of controlling their own information space, and subverting those of their adversaries, in what they see as an ongoing conflict of ideas with the West. It is therefore just as much an arm of those states' propaganda machines, and a means of creating and delivering 'fake news', as it is a means of penetrating an adversary's critical infrastructure. In one sense this gives both China and Russia the advantage of having a more integrated approach to how cyber capability is employed as part of a wider geopolitical strategy. But this doctrinal difference may have resulted in China and Russia devoting fewer resources than the US to developing the types of military offensive cyber capability that are designed surgically to bring down sophisticated critical civilian and military networks during an armed conflict. Russia's attempts in the United Nations to outlaw such 'military' capabilities, and its use of relatively blunt tools such as NotPetya against Ukraine, may be indicators of this asymmetry in capability.

What sets the US apart on offensive cyber is its ability to employ a sophisticated, surgical capability at scale. It has the advantage of being the global first mover, having invested earlier and more heavily than China and Russia in the underpinnings of cyber power. US offensive cyber potential also benefits from close alliances with other cyber-capable states. Notably, the sophisticated cyber operation to disrupt Iranian nuclear enrichment, revealed in 2010, was only midway through approximately 25 years of experience that the US has accumulated. That said, offensive cyber operations do not need to be sophisticated to achieve strategic effect. Iran and North Korea, operating alone, have been able to develop and use relatively unsophisticated techniques against neighbouring countries. They have also reached beyond their regions, including into the mainland US, in ways that their conventional capabilities cannot achieve. Russia's interference in US democratic processes is another prime example of successful use of unsophisticated cyber operations. This means that during the last decade, given its different doctrinal approach and greater regard for legal and ethical constraints, the US is more likely to have been the victim of an offensive cyber attack than the perpetrator. The US may be the most powerful cyber state, but arguably other countries are making greater use of their cyber capabilities in order to exert power. This probably explains the US doctrinal shift in 2018 to the Cyber Deterrence Initiative – a component of which is an attempt to transfer the day-to-day contest from its own networks to those of its perceived adversaries.

International dialogue and agreement on the use of offensive cyber capabilities is sparse, given the sensitivity of the capabilities involved. Overarching cyber norms of behaviour (non-binding and voluntary) have been developed under UN auspices, with the norm attempting to limit the targeting of critical national infrastructure of particular relevance.[7] In 2020, work led by the International Committee of the Red Cross started to focus on further defining a responsible state use of offensive cyber. This work differentiates between the surgical and controlled use of sophisticated tools designed to minimise collateral damage (as with Stuxnet) and, for example, the uncontrolled exploitation of global IT vulnerabilities with little thought given to the likelihood of widespread collateral damage (as with NotPetya and WannaCry). These, though, are exceptions that prove the rule. Generally, in order to manage the risks of uncontrolled proliferation and escalation, more common ground needs to be found for inter-state dialogue on offensive cyber. This will involve states thinking creatively about how they balance greater transparency with the understandable need to protect sensitive national capability.

Resources

In trying to measure cyber power, it is necessary to assess the inputs, such as human capital (numbers of people), money invested and the quality of technologies used.

However, in the case of every country, the number of people allocated to cyber roles is difficult to gauge. Published figures often cover only dedicated cybersecurity professionals in specialist government agencies and do not take account of wider public- and private-sector capacity. Measuring the size of the effort dedicated to military effect is particularly difficult. The US military has indicated the size of its dedicated cyber units, but

such raw numbers (6,000 in the case of Cyber Command, for example) do not include the large workforce involved in support roles, especially intelligence collection, in agencies with broader functions. All countries rely on close partnerships between the armed forces, civilian agencies and the private sector, and these are delivered in different ways and proportions by each country. In the cases of China and Russia, we may know their approximate numbers of dedicated information-warfare personnel but we should not count all of these as cyber, as an unknown proportion of them undertake more intelligence-related or traditional information-warfare roles that do not require cyber means. We also cannot easily distinguish between the numbers of people allocated exclusively to cyber espionage and those allocated to non-espionage military cyber operations. Nevertheless, the published strategies, doctrines and plans of the US, China and Russia indicate that they are likely to have the largest numbers of personnel dedicated to military cyber operations (mostly espionage), with personnel strength amplified particularly in the US by the large number of people with cyber-relevant skills who are employed in the private sector.

However, in cyber operations, while numbers can make a difference, the crucial factor is skills (indeed, one highly skilled individual could defeat an inadequately trained cyber division of 10,000). Every cyber-capable country, whether authoritarian or liberal-democratic, has therefore identified skills shortages as a major risk. Each has embarked on upskilling and training initiatives, although, as our country studies indicate, cyber-related research and education appear to be stronger in the liberal-democratic states. From a cyber perspective, the education systems of China and Russia remain relatively underdeveloped, as do those of Iran and North Korea.

The size of financial investment in cyber capabilities is also hard to measure, for the same reasons. But again, the studies suggest that the investments by the US, China and Russia are the largest. As a proportion of GDP, and taking into account their growing cyber-related private sectors and academia, investment by the UK and Israel also looks significant. It is notable that Chinese specialists regularly bemoan the low proportion of GDP that their country spends on cyber security in comparison with the US.

While attempting some estimate of the human and physical resources is important, we also acknowledge that the principal determinants of a state's ability to exploit cyber power are political will and the quality of the cyber operations that are tailored to those particular political objectives. These are human factors and they are not easily quantified; indeed, in most cases they are not even observable.

International alliances

What individual countries lack in terms of resources and expertise, they may be able to make up for through international alliances. The dominant cyber alliance is without doubt the one built on the 65-year-old Five Eyes intelligence partnership. All five countries are individually cyber-capable – with the US the most capable of all – but they each gain significantly from the alliance. France, Israel and Japan are among the other states that also have mutually beneficial cyber alliances with individual Five Eyes members. China, Iran, North Korea and Russia, meanwhile, do not have a meaningful cyber alliance either with each other or with any other state.

Military transformation

Several states have moved decisively to transform their military strategies, doctrines and structures to recognise both the opportunities and the threats created by cyberspace technologies. Leading states, particularly the US and China, envisage future warfare being won and lost in a cyberspace enabled by artificial intelligence and space platforms.

Several factors have shaped those transformations, including the scale of cyber vulnerability in legacy systems, national cyber-industrial and skills potential, the extent of reliance on civilian intelligence capability, leadership commitment, and resistance from military traditionalists. No state has yet made a transition in its current armed forces to well-integrated and broadly dispersed cyber capabilities, either for defensive or offensive purposes. The US has probably gone furthest. One implication of this gradual and only partial transition is that the full potential of military cyber power in the medium term – in the 2030s, say – has yet to be demonstrated in practice.

Strategic shock

The expanding development and use of cyber capabilities by states has to some extent been escalated by strategic shocks**.** The first of these came in 1991, during the First Gulf War, when the US proved capable of integrating intelligence and precision-guided weapons to a degree that China and Russia had not yet imagined. US operations in 1999 against the Federal Republic of Yugoslavia's forces in Kosovo had a similar shock effect, as described in subsequent speeches by then Chinese president Jiang Zemin. Several senior US military figures have alluded to the offensive cyber operations that formed part of that campaign. Later, the presumed use of cyber tools in US military operations in Iraq in 2003 attracted widespread attention, as did the perceived role of the internet in the various so-called 'colour revolutions' of the 2000s in Georgia, Kyrgyzstan and Ukraine. As a result of their perceived relative vulnerabilities, China and Russia began pushing via the UN, as early as 2003, for greater state control over their 'sovereign' cyberspace.

Arguably the biggest shock was still to come, however: the 2013 Edward Snowden leaks, with their revelations about the extent and sophistication of US and allied cyber capabilities, including the role played by leading US digital companies in enabling intelligence collection. China and Russia were at the same time creating their own shocks in cyberspace – most famously the Chinese theft of Western intellectual property on an industrial scale, which had been tracked since at least 2011, and the attempted Russian interference in US democratic processes, which began in 2014 and escalated in 2016. These in turn led the US to shift to the strategy of 'persistent engagement' and 'defend forward' under its Cyber Deterrence Initiative, exemplified by the reported 'strike back' in 2018 against a Russian hacking group, the Internet Research Agency, in the run-up to the US midterm elections. Russia's intelligence-gathering hack into the US ICT supply chain, discovered in late 2020 – the SolarWinds hack – seems to have been on a scale sufficient to constitute another strategic shock.

The story for Iran is similar, with its development of defensive cyber capabilities accelerated by its perception of the role played by the internet in the Arab Spring of 2010–11 and in its own internal unrest (the Green Movement of 2009, for example). Its development and use of offensive capabilities, for example against Saudi Aramco, was direct retaliation for the shock of the Stuxnet hack into its nuclear-enrichment programme.

Tiering

Using the methodology to rank the 15 countries by cyber capability, we identify three broad tiers. Tier One: world-leading strengths in all the categories in the methodology. Tier Two: world-leading strengths in some of the categories. Tier Three: strengths or potential strengths in some of the categories but significant weaknesses in others. There are also cyber weaknesses among the states in Tier Two, and even in Tier One, but they are minor when compared with the significant weaknesses that consign states to Tier Three. We have drawn the following broad conclusions.

The **US** remains the most cyber-capable state. Since the mid-1990s its leaders have provided clear political direction for the pursuit of national cyber power: in that time it has invested heavily in developing relevant civilian and military capabilities, gained extensive operational experience and developed the world's strongest digital-industrial base. This is highlighted by the range of US companies capable of detecting and attributing state cyber attacks and the proven sophistication of the US offensive cyber capability, military or otherwise. US cyber strength is also founded on a world-class cyber-intelligence capability with global reach and state-of-the-art cryptographic techniques, and is amplified by highly integrated partnerships with other states that are also among the most cyber-capable in the world. Nevertheless, the ways in which the US wields its cyber power appear politically and legally constrained when compared with its main cyber adversaries – Russia, China, Iran and North Korea. The US has sought to be a responsible offensive cyber actor, governed by international law and at pains to limit potential collateral damage. It has also sought to manage its degree of dependence on cyberspace, not only for the purpose of national security but also for economic and political reasons. This challenge is exacerbated by the complexity of its cyber governance and command-and-control structures, where the large number of agencies involved is a potential impediment to the agility of operational

decision-making. These factors have combined to give the adversaries of the US an edge in the use of unsophisticated cyber techniques that are aimed at subversion but pitched below the legal threshold for an act of aggression that might justify an armed response. Doctrinal shifts such as persistent engagement and defend forward are designed to redress this imbalance. Nevertheless, the US performs strongly across all categories of the methodology and is alone in Tier One.

Below the US there is a second tier of seven countries: in alphabetical order they are Australia, Canada, China, France, Israel, Russia and the UK. Each has world-leading strengths in some of the categories in the methodology.

Compared with the other countries in the second tier, the **UK** and **Israel** are particularly strong on cyber security, core cyber-intelligence (including cryptographic) capability, and the development and use of sophisticated offensive cyber capability. With clear political direction, both benefit from a whole-of-society approach to cyber security with a strong and growing cyber-security industrial base and innovative approaches to increasing their skilled capacity. They also possess a vibrant technical-innovation and start-up ecosystem. Israel's cyber-intelligence strength appears to be heavily focused on its region, where it has no equal. The evidence indicates that the UK, on the other hand, has a cyber-intelligence capability with a broader, worldwide reach. The UK also has two of the 51 tech or telecoms companies that appear in the 2020 *Fortune* Global 500, while Israel has none.[8] Both countries lag behind the US, Japan, China and others in their capacity to build future internet infrastructure; both compensate for a comparative lack of cyber mass through close partnerships with the US, with each other and with other cyber-capable nations; and both have conducted offensive cyber operations jointly with the US.

France is also particularly strong on cyber security and has a wide intelligence reach. But these capabilities, together with French offensive cyber, probably lag behind those of the US and the UK in terms of strength and depth, given France's surprise at the Five Eyes capability revealed by Snowden. One contributory factor may be that, unlike all the other countries in this second tier, France keeps its cyber security organisationally separate from its cyber intelligence and offensive cyber. While the French desire for national autonomy on intelligence may also have limited its progress in some areas, this can be considered a strength when compared with countries that are overly dependent on international alliances for cyber mass. France has only one representative among the 51 tech or telecoms companies in the 2020 *Fortune* Global 500.

Canada has a particularly strong digital economy, with a vibrant technical start-up ecosystem. It is one of the world leaders on cyber security, founded on creative partnering between its public and private sectors and an innovative approach to developing skills. For Canada, and also for **Australia**, membership of the Five Eyes alliance is seen as a key means of compensating for any shortfall in indigenous capability. Canada's development and use of offensive cyber capabilities remains nascent, however, whereas Australia has a developed capability that it has used, for example, in joint operations with the US and the UK. Australia is trying to boost its cyber-security and tech sectors, in which it is starting from a lower base than Canada. Neither Canada nor Australia has a representative among the 51 tech/telecoms companies in the 2020 *Fortune* Global 500.

China and **Russia** both lag behind the Five Eyes nations, and Israel and France, in terms of cyber security. Evidence for this comes from their own internal reports, their low rankings in the ITU Global Cybersecurity Index, their push at the UN since 2003 for greater state control of sovereign cyberspace and their pursuit of some technical isolation from the global internet (with China seemingly further ahead than Russia in this regard). A contributory factor may be the comparative immaturity of their cyber-security industries and their low skills bases. That said, both may have secretly improved their defensive capabilities in response to the 2013 Snowden revelations, although it is worth noting that particularly damning internal reports on the state of China's cyber security were produced in 2017 and 2018.

In their development of offensive cyber mass, the scale of their respective operational experience, their proven reach on cyber espionage and the clarity of their political direction and doctrinal thinking, China and Russia probably surpass all other states except the US. Furthermore, their adoption of cyber techniques for mass

influence and subversion as part of wider information campaigns against adversaries is arguably without parallel. But the degree to which both Russian and Chinese cyber operations are detected and attributed, particularly by specialist Western companies, raises important questions. It is difficult to ascertain whether the detection of those operations is mainly the result of their lacking the highest levels of technical sophistication and employing poor tradecraft, whether China and Russia care less than Five Eyes countries about getting caught, or even whether other, more sophisticated capabilities may be concealed in the sheer volume of activity. Finally, while none of the 51 tech/telecoms companies in the 2020 *Fortune* Global 500 are Russian, eight are Chinese, and that number will probably rise in coming years. This means that overall, despite questions about its cyber security, China is the only state currently on a trajectory to join the US in the first tier of cyber powers. This trajectory might be slowed by the moves the US has made since 2019 to close its markets, and those of its allies, to certain Chinese digital companies. However, China has two distinct advantages: it is home to one billion of the world's estimated four-and-a-half billion internet users (more than the US and Europe combined); and the comparative cheapness of Chinese technology makes it attractive to developing countries, especially those inclined to use it for internal surveillance. China is attempting to exploit the latter advantage under the Digital Silk Road component of its Belt and Road Initiative.

Of the 15 countries assessed in this report, seven are in a third tier. These countries are at much earlier stages in their cyber journeys, each having strengths or potential strengths in some of the categories in the methodology but significant weaknesses in others. A more granular ranking within this third tier could cut several ways, depending on which of the categories in the methodology are deemed the most important. Below, the countries are simply listed in alphabetical order.

India has a large digital economy but, as in other areas, its complex bureaucracy slows its advance in cyber security, leaving it in a low position in the ITU's Global Cybersecurity Index. The country has some cyber-intelligence and offensive cyber capabilities but they are regionally focused, principally on Pakistan. It is currently aiming to compensate for its weaknesses by building new capability with the help of key international partners – including the US, the UK and France – and by looking to concerted international action to develop norms of restraint.

Indonesia has ambitious plans to develop its digital economy (only 73% of Indonesians currently use the internet) but is a late starter on cyber security, with progress slow in the face of the major threats it faces from cyber crime and cyber-based terrorist propaganda. Its cyber-intelligence capabilities are well developed for internal surveillance but are embryonic elsewhere, as too is its offensive cyber capability.

Iran has used relatively unsophisticated offensive cyber capabilities for diverse goals: to counter domestic subversion, for its own subversive operations abroad and for power projection. In doing so, it has shown a relatively high level of operational maturity and a clear leadership embrace of cyber operations as useful instruments of power, allowing it to reach outside its immediate region in ways that are beyond its more conventional capabilities. Iran's cyber capabilities are amplified by its use of internal proxies such as the Mabna Institute and the Iranian Cyber Army. Iran has also provided some cyber tools and training to its favoured external partner, Hizbullah. However, Iran almost certainly lacks any high-intensity-warfare-grade offensive cyber capability. The ITU has listed a range of Iranian deficiencies on cyber security, giving the country a low position in its cyber-security index. Iran's population is increasingly internet-dependent, with the government aiming to provide certain services entirely online, but generally the country lacks digital resilience and contingency preparedness owing to technological, organisational and economic deficiencies. It is aiming for a strategic solution by investing heavily in creating its own national internet platform – but, despite its claims to the contrary, that is not a near-term prospect. Iranian cyber-intelligence capabilities are strong regionally, and may have benefited from some intelligence cooperation with Russia during the war in Syria.

Japan has the advantage of a world-leading internet-related high-tech industry. It has ten of the 51 tech/telecoms companies in the 2020 *Fortune* Global 500 – ahead of China and Western Europe, and second only to the US. But its cyber-security capability is not strong,

and it is now seeking to compensate for that by closer partnerships with the US and others. For constitutional reasons, Japan has so far developed no offensive cyber capability. There are indications, however, that it may be willing to reconsider how its constitutional boundaries apply to the cyber domain.

Malaysia was the first member of the Association of Southeast Asian Nations to move strongly on cyber-security policy and to focus on expanding its ICT sector. It remains highly regarded for its policies and its international leadership in cyberspace affairs, but it does not make a strong contribution to the global ICT sector. There is little evidence of either core cyber-intelligence capabilities or the development of offensive cyber.

North Korea has shown itself capable of significant harassment in cyberspace. It has used a proto-criminal modus operandi to conduct large-scale cyber fraud and extortion; to steal intellectual property and intimidate other states in its region, especially South Korea; and occasionally also for sabotage – either deliberate, as with Sony Pictures in 2014, or accidental, as with WannaCry in 2017, when it lost control of a capability. But it lacks any sophisticated offensive cyber or cyber-intelligence capability, and its cyber security is assessed by the ITU to be among the weakest in the world. Generally, given its isolation, North Korea is hampered by a low cyber-skill base, even though (contrary to popular belief) it has at least four million devices connected to internal 3G mobile networks, its government operates an intranet, and parts of its critical national infrastructure rely on internet connectivity. Its connections to the global internet are limited, rely on Chinese and Russian service providers, and are highly vulnerable to disruption. This means the country is often obliged to deploy its operators abroad in order to deliver any type of cyber effect.

Vietnam has prioritised the development of its ICT sector and the construction of e-government platforms. Although policies surrounding information security have been published and basic cyber-security structures established, the fact that a comprehensive national cyber-security strategy remains unpublished both undermines the potential mobilisation of key stakeholders and limits its public awareness. Government agencies still grapple with cyber-security issues owing to limited budgets and a severe shortage of cyber-security talent. The ruling Communist Party of Vietnam's fear of internal subversive threats may also tend to draw resources away from technical cyber-skills training towards ideological work and the management of public opinion, reducing the focus on the development of either defensive or offensive cyber capabilities. To realise its digital ambitions Vietnam needs to strengthen training in cyber security, prioritise support for domestic ICT firms and invest in more advanced technologies for cyber security.

Moving up

Of all the factors potentially contributing to a country moving up from one tier to the next, the most decisive appears to be strength in the core ICT industries. That is why China, on its current trajectory and providing it addresses its weakness in cyber security, is best placed to join the US in Tier One. It is also why Japan, despite the many weaknesses it needs to address, is the Tier Three country best placed to rise into Tier Two.

Notes

1 For a discussion of the challenges, see Eileen Decker, 'Full Count? Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score', *Journal of National Security Law & Policy*, vol. 10, no. 3, 13 February 2020, pp. 583–604, https://jnslp.com/wp-content/uploads/2020/05/Crime-Rate-Swings-Cybercrime-Misses.pdf.

2 See, for example, Ross Anderson et al., 'Measuring the changing cost of cybercrime', paper presented to the 2019 workshop 'Economics of Information Security', Boston, US, 3–4 June 2019, pp. 5–8, http://orca.cf.ac.uk/122684/1/Levi_Measuring%20the%20Changing%20Cost%20of%20Cybercrime.pdf.

3 The US government's Clean Network programme is aimed at protecting US citizens' privacy and US companies' most sensitive information 'from aggressive intrusions by malign

actors, such as the Chinese Communist Party'. See US Department of State, 'Announcing the Expansion of the Clean Network to Safeguard America's Assets', 5 August 2020, https://china.usembassy-china.org.cn/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets.

4 Because AI research is largely a globalised enterprise, attributing nationality to it is not easy. There are discrete sub-fields (up to ten, depending on one's perspective) and more than 20 sectors of economic and social activity to which those sub-fields can be applied. The US leads the world by a wide margin in AI applications for the health sector, and China may well rank quite highly in AI applications for energy efficiency. Moreover, as the Organisation for Economic Co-operation and Development (OECD) has noted, every country has its own distinct priorities and enablers when it comes to exploiting AI for economic gain – see OECD, *Artificial Intelligence in Society* (Paris: OECD Publishing, 2019), https://doi.org/10.1787/eedfee77-en. The same caution about over-generalisation applies to the use of AI for national-security or military purposes.

5 We decided to examine four developing cyber states from roughly the same region of the world, choosing South and Southeast Asia.

6 For the tech companies in the 2020 *Fortune* Global 500 ranking, see https://fortune.com/global500/2020/search/?sector=Technology. For the telecoms companies, see https://fortune.com/global500/2020/search/?sector=Telecommunications.

7 Agreement was reached in 2015 within a Group of Governmental Experts appointed by the UN General Assembly on possible voluntary norms governing international behaviour of states in cyberspace. The relevant UN document is Secretary-General, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/70/174, 22 July 2015, https://undocs.org/A/70/174.

8 See the lists of the leading tech and telecoms companies among the 2020 *Fortune* Global 500: https://fortune.com/global500/2020/search/?sector=Technology and https://fortune.com/global500/2020/search/?sector=Telecommunications respectively.

1. United States

Dominance in cyberspace has been a strategic goal of the United States since the mid-1990s. It is the only country with a heavy global footprint in both civil and military uses of cyberspace, although it now perceives itself as seriously threatened by China and Russia in that domain. In response, it is taking a robust and urgent approach to extending its capabilities for cyber operations, both for systems security at home and for its ambitions abroad in the diplomatic, political, economic and military spheres. The US retains a clear superiority over all other countries in terms of its ICT empowerment, but this is not a monopoly position. At least six European or Asian countries command leadership positions in certain aspects of the ICT sector, though all but one (China) are close US allies or strategic partners. The US has moved more effectively than any other country to defend its critical national infrastructure in cyberspace but recognises that the task is extremely difficult and that major weaknesses remain. This is one reason why the country has for more than two decades taken a leading role in mobilising the global community to develop common security principles in cyberspace. The US capability for offensive cyber operations is probably more developed than that of any other country, although its full potential remains largely undemonstrated.

Strategy and doctrine

The United States has a series of well-developed national strategies for defence and security in cyberspace that has been maturing for more than 30 years. There are three broad directions: homeland defence, low-intensity conflict and high-intensity war. These are captured in relevant sections of the 2017 'National Security Strategy of the United States',[1] the 2018 'Cyber Strategy of the United States'[2] and the 2018 'Department of Defense Cyber Strategy'.[3] These are supported by policy statements and doctrine manuals that run to several thousand pages.

To complement and buttress the national-security strategies, the US has also been developing its civil-sector cyber-security policy since the mid-1990s, initially with a focus on countering cyber crime and preventing losses to the corporate sector. Its formal strategy of 2018 has been followed by a very large number of executive orders (including one on former president Donald Trump's penultimate day in office),[4] policy statements, action plans and other decisions. Throughout the last three decades there has been a sharp and intensifying concern

List of acronyms

CDI	Cyber Deterrence Initiative
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
ICT	information and communications technology
ISAC	Information Sharing and Analysis Center
ITU	International Telecommunication Union
NSA	National Security Agency
NSC	National Security Council
ODNI	Office of the Director of National Intelligence

about protecting the country's critical information infrastructure (the cyber aspects of what most other countries simply refer to as 'critical infrastructure' or, as in the United Kingdom, 'critical national infrastructure').[5] Key stakeholders (business, academics, government, state authorities, defence interests, the National Guard and privacy-protection groups) have become highly mobilised around ensuring an integrated national response, covering the human as well as the technical challenges involved in improving cyber security.

The concern has been to plug the gaps that had resulted in spectacular leaks of state secrets, theft of intellectual property, foreign interference through cyberspace in US politics, and the poor cyber-security performance of many sectors of the economy and society.

In military affairs, the US aims to provide cyber-attack options in all phases of operations and at every level of command.[6] On the defensive side, the aim is to ensure that cyber defences are wide-ranging, robust and highly resilient. In both regards the US has made more progress than any other country. However, in the event of a major conflict, it remains the case that the US – including its military – could be severely damaged by cyber attacks, given the country's high degree of digital dependence. Comprehensive defence in cyberspace would be difficult or perhaps impossible to ensure in wartime.[7]

The US international strategy for cyberspace in peace and war – as framed by the head of US Cyber Command, General Paul Nakasone – is to 'achieve and maintain cyberspace superiority'.[8] This formulation also precisely captures the intention of the country's political leaders. The 2018 Department of Defense (DoD) strategy for cyberspace offers additional detail.[9] In it, the US Joint Chiefs of Staff set near-term objectives that recognise the limitations of current cyberspace capabilities, both offensive and defensive, with a clear view that offensive cyber operations will be directed towards maximising existing advantages, whether kinetic or informational.

Since the main positive impact of extensive and detailed planning for cyberspace operations is the potential for nationwide mobilisation of resources, both for daily operations and emergencies, the US is clearly in a highly advanced position in this regard. The strategies and policies are comprehensive, as well as widely and effectively disseminated. Significant sections of government, the armed forces, the business community, civil society and academia are engaged in developing those strategies and executing them. The strategies also recognise how rapidly the circumstances of cyberspace are changing and the huge complexities that must be overcome in exploiting adversary weaknesses. The speed at which the cyber threat has continued to evolve has proven highly disruptive even to a policy process as advanced as that of the US.

A key component of the 2018 cyber strategy is its Cyber Deterrence Initiative (CDI).[10] This states that the US will work closely with allies in responding to cyber attacks (including through intelligence-sharing), attributing attacks, formulating public statements of support for actions taken and jointly imposing consequences against those responsible. While the national cyber strategy makes it clear that there are many non-cyber ways to retaliate, the 2018 DoD strategy sets out the role US cyber operations are intended to play in assertively defending national interests. These include 'defending forward' on adversary networks in order to pre-empt attacks, and competing constantly with adversary cyber operators ('persistent engagement').

Cyber governance in the US is highly pluralistic

Governance, command and control

The US has been a world leader in promoting and practising multi-stakeholder governance of security in cyberspace, doing so in a way that owes much to its liberal political culture and institutions and to robust opposition by the corporate sector to regulation of private businesses. The latter factor is particularly relevant to the protection of critical infrastructure since most of it is in the hands of private businesses. The federal character of the national political system assigns to the 50 states, alongside other small political entities and administrations, significant roles in national cyber security, especially in countering cyber crime and in education. Cyber governance in the US is highly pluralistic.

In US cyber policy there are many channels of executive authority that flow from the president: the intelligence community, the armed forces, departments of state (Homeland Security, Defense, Justice, Commerce, Energy and Transport) and other agencies (such as National Laboratories). These are all coordinated through the National Security Council (NSC), chaired by the president, and its Principals Committee, chaired by the national security advisor.[11]

For civil-sector cyber security, the federal government has had two main channels for its policymaking. The first is in the White House, through the cyber director on the staff of the NSC. The president is directly supported by the homeland security advisor (serving under the national security advisor) and a deputy national security advisor for cyber security and emerging technology.[12] The second channel is outside the White House, through the secretary of the Department of Homeland Security (DHS), a full member of the NSC, and a new organisation set up in 2018 under DHS, the Cybersecurity and Infrastructure Security Agency (CISA).

These agencies rely on a long-standing policy of mobilising (or sometimes effectively co-opting) private-sector and public participation in their initiatives. One vehicle for this has been the president's National Infrastructure Advisory Council, which brings together senior executives from the private sector and state and local governments to advise on how to reduce 'physical and cyber risks and improve the security and resilience of the nation's critical infrastructure sectors'.[13] The agencies have introduced a range of strategic initiatives, including the Information Sharing and Analysis Centers (ISACs),[14] the first of which was created during the presidency of Bill Clinton; the Cyber Risk and Resilience Review framework,[15] jointly devised in 2009 by the DHS and Carnegie Mellon University; and the National Initiative for Cybersecurity Education, an organisation within the National Institute of Standards and Technology in the Department of Commerce.

In the development of command and control for cyber operations, two main trends have been discernible: a filling of policy gaps through the creation of new organisations and/or posts for a wide range of missions and responsibilities, and a gradual decentralisation of authority for offensive operations. The unifying purpose has been to improve the capability and effectiveness of defence and offence in cyberspace. The US has invested heavily in these changes. For the 2021 fiscal year the government requested US$18.7 billion for specific security initiatives.[16]

For national-security policy in cyberspace, there are many departments and agencies involved in authorising, commanding and controlling cyber operations. In addition to the White House and DHS, the most important are the DoD, as it contains the National Security Agency (NSA) and Cyber Command; the State Department; the Office of the Director of National Intelligence (ODNI), which coordinates all the intelligence agencies; and the Central Intelligence Agency (CIA), which reports directly to the president while coordinating with the DNI.

For military planning and operations, the command-and-control arrangements match those of all military activities. The president is the commander-in-chief, to whom the unified (theatre/domain) commands and the single-service chiefs (army, navy, air force and marines) report. The function of commander-in-chief is exercised through the secretary of defense, under a mechanism called the National Command Authority. In 2012, then-president Barack Obama ordered that offensive cyber operations conducted by the military required multi-agency agreement and presidential authorisation. In 2018, in response to sustained cyber attacks on the US below the threshold of armed conflict, then-president Trump approved the CDI and in a classified directive provided for the devolution of authority for offensive cyber operations to various agencies in certain cases.

Within the DoD, the list of cyber agencies with operational and capability-development roles is a long one, including single-service cyber commands and the DoD chief information officer, responsible for securing all DoD computerised systems (not including deployed weapons platforms, which are managed by the single-service cyber commands or combatant commands).

Governance of cyber policy in the US is enriched by the diversity of talents and interests represented in the various powerful institutions that are involved. Policy is inevitably consensus-based and therefore perhaps less focused than in other, less pluralistic systems, but

there is larger buy-in by stakeholders throughout the US system. Since it is based on strict observance of the law, the US system is highly predictable, though therefore more constrained than in countries where the law is less respected or more arbitrary. Command-and-control arrangements are worked out in exquisite detail, with high levels of redundancy built in, and with command nodes enjoying a high degree of intelligence support.

Core cyber-intelligence capability

There is copious public evidence indicating the world-leading sophistication, breadth and depth of US core cyber-intelligence capabilities. These are centred on the extensive military-led cyber capabilities of the NSA, the complementary civilian-led cyber capabilities of the CIA, with its covert overseas remit, and those of the Federal Bureau of Investigation (FBI), with its domestic-security remit. The director of the NSA also heads the US military's Cyber Command, and both organisations have cyber-intelligence, cyber-security and offensive cyber functions so as to maximise the synergies across such closely related activities. Core US cyber-intelligence capabilities are enhanced further through many international intelligence partnerships, with the long-established Five Eyes alliance as the centrepiece. The Five Eyes is arguably the most powerful international intelligence partnership in history.

The US intelligence agencies collaborate extensively with private-sector firms and universities for the development and evaluation of key technologies.[17] The extent of civil–military and private–public integration can be seen in the March 2019 report by the National Academies of Sciences, Engineering, and Medicine on the future directions the intelligence community could take in order to adapt to, or exploit, rapidly changing technologies.[18] The very tight integration of government, industry and academia in shaping the US intelligence capability is unmatched in scale, focus and investment by any other country, including China. The country's cyber-intelligence capability also benefits from the maturity and scope of the centralised process for all-source intelligence fusion and assessment.

With an annual budget request of US$85bn for the 2021 fiscal year, and the involvement of multiple government departments in addition to the three core intelligence agencies, the size and complexity of the US intelligence-and-security community make it notoriously difficult to coordinate, even following the post-9/11 creation of the ODNI, which was designed to address the problem.

Cyber empowerment and dependence

The US remains the most powerful country in terms of ICT capability, whether gauged by the size of its digital economy, its leading role in global innovation or the unrivalled partnership between industry, government and academia. Global consumer demand for US ICT has led to the unprecedented commercial success of companies such as Apple, Google and Microsoft, which has in turn stimulated their shaping of the future of cyberspace through their extensive investment in research and development (R&D). The result is a high degree of global dependence on US commercial products and intellectual property, with the technology involved in computer microchips, undersea communication cables, communication satellites and cloud computing being prime examples. The other side of the coin is that the US economy and civil infrastructure are more dependent on cyberspace than those of most other countries, and therefore more vulnerable in many respects.[19]

The US is a world leader in both personal and business use of the internet and mobile technology. The level of demand has contributed to domestic innovation, which has in turn fuelled even higher demand. The US digital economy is the biggest in the world.

According to the standard methods used by the US government's Bureau of Economic Analysis, the digital economy contributed 9% of the country's GDP in 2018.[20] But this estimate excludes the output of sectors where large amounts of wealth are generated by ICT products and services, such as financial services. It is not possible to gauge the full strength of the US digital and cyber economy just by using the traditional ICT output data from the national accounts for the ICT sector.[21] Other sectors of the US economy – such as agriculture, banking and healthcare – leverage ICT goods and services to create their own innovations and wealth in ways that are not included in national statistics for the ICT sector.[22]

For example, every day in the US, trillions of dollars' worth of financial transactions are conducted in ways that are only possible because of ICT systems.[23] One of

the favoured techniques is algorithmic trading of stocks, derivatives and currency, where ICT systems are pre-set to buy and sell according to certain pre-determined parameters. This has resulted in a new form of automated, high-speed wealth creation, making the US the global centre for 'digital capitalism'.[24] Using the broader measure of the digital economy adopted by the G20,[25] the digital economy's share of US GDP is about 60%.[26]

Overall, it is clear that the US enjoys a significant level of cyber empowerment compared with all other countries. Some countries, including China, aspire to emulate US achievements in this regard. In fact, between 2013 and 2016, according to an estimate by the Organisation for Economic Co-operation and Development (OECD), China was already one of the five countries – together with the US, Taiwan, Japan and South Korea – that together produced at least 70%, and in some cases almost 100%, of the patents for each of the 25 new technologies considered by the OECD to represent the 'digital technology frontier'.[27] However, the US share of global production was greater than China's for all but two of those technologies (control arrangements and organic-materials devices).[28]

The strength of US digital services lies largely in their culture of technical expertise and innovation-led investment. The US is home to 59 of the universities in the *Times Higher Education* list of the global top 200 (see Table 1.1, which includes only the countries that feature in this report), and its tech and entrepreneurship ecosystem has no equal. According to one industry survey, there were 65,321 start-ups listed in the US in 2019, which was approximately nine times the number in the second-placed country, India.[29]

Table 1.1. **Universities in the *Times Higher Education* global top 200, 2021**[30]

US	59
UK	29
China (incl. Hong Kong)	12
Australia	12
Canada	8
France	5
Japan	2
Israel	1

Private investment in the US high-tech sector has been a central part of this dominance in a way not matched by any other country. In 2019, the available data suggested that total venture-capital investment in the US was more than three times greater than in China (US$135bn versus US$40bn).[31] In the 2020 IMD World Competitiveness Ranking, which assesses a country's ability to 'adopt and explore digital technologies' across government, business and wider society, the US was in tenth place and China was in 20th.[32] According to the United Nations Conference on Trade and Development, the US accounts for 68% of the market-capitalisation value of the world's 70 largest digital platforms, compared with China's 22%.[33] In terms of its share of total global spending on R&D, using a purchasing-power-parity estimate, the US was in first place in 2019, just ahead of China.[34] Taking the last two decades as a whole, the gap between the two countries is much wider, with US R&D investment almost double that of China, and the impact of that earlier spending remains significant today.

Taking investment in and outputs from research in the field of artificial intelligence (AI) as an important proxy indicator of cyber empowerment, we can see several trends. Between 2008 and 2017, US venture-capital investments in AI outpaced those in China (US$694bn versus US$185bn).[35] China overtook the US in 2018, but later that year its entire venture-capital sector suffered a collapse. In terms of research, in 2016 the 28 European Union member states and the US were responsible for the two greatest shares of highly cited AI-related publications, 23% and 15% respectively, but those shares declined to 17% and 12% in 2018.[36] China overtook both, with a share of 28% in 2018, while India's share skyrocketed to 11%. (Note, however, that this ranking demonstrates scientific achievement rather than economic power, since open-source publications are available to be used in any country, not just the one in which they were produced. And in most cases the researchers producing such publications are likely to include some foreigners, so in that sense the scientific achievement does not belong entirely to the source country.) Overall, the statistics do not capture the quality and dynamism of the US AI sector, which was demonstrated in 2018, for example, by the Massachusetts Institute of Technology's creation of a special school of

computer science for the purpose of developing the AI-related research of non-IT departments.[37]

In February 2019, Trump announced a national AI initiative (two years after China had done so), saying that 'continued American leadership in AI is of paramount importance to maintaining the economic and national security of the United States and to shaping the global evolution of AI in a manner consistent with our nation's values, policies, and priorities'.[38] In 2020, the government reported that it was on track to double its investment in non-defence AI by 2022, including through the allocation of US$850 million for AI activities at the National Science Foundation.[39]

The global footprint of US-based telecoms and high-tech companies is also very large, one example being the ownership and repair arrangements for global undersea communications cables.[40] Google is the biggest single owner of undersea cables, and US corporations have 36 representatives among the 169 members of the International Cable Protection Committee, compared with China's one.[41] The US has identified foreign-based cable-landing stations, including several in China, as part of its own critical national infrastructure.[42] How it would respond to any Chinese government interference with those installations is uncertain.

In terms of space connectivity, the US operates at least three times as many satellites as China (see Table 1.2, which includes only the countries that feature in this report). US military cyber activity is heavily dependent on its space assets, since the vast majority of military cyber activity is executed via outer space – especially intelligence collection, damage assessment and targeting.

Table 1.2. **Numbers of satellites (January 2021)**[43]

US	1,897
China	410
Russia	176
UK	167
Japan	84
India	63
Canada	43
France	22
Israel	16
Australia	13
Indonesia	9
Malaysia	5
Vietnam	4
Iran	2

The US also remains dominant in the manufacturing of computer chips (see Table 1.3), an essential component in all modern computing. Not only does it have by far the largest share of the global market, but US companies that design, manufacture and sell semiconductors – so-called integrated device manufacturers – account for 51% of global sales.

Table 1.3. **National semiconductor industries' share of global market (%), 2020**[44]

Country	Type of semiconductor			
	Logic	Analogue	Memory	Discrete
US	61	63	23	23
South Korea	6		65	5
Europe	9	22		42
Japan	6	9	9	25
China	9			5
Taiwan	9		3	

However, for all its digital economic power, the US relies on a globalised market and supply chain. This played out in private-sector complaints against the Trump administration regarding its efforts to ban companies around the world from relying on computer chips manufactured wholly or even partly in China, as part of a multinational supply chain.[45] Many tech and telecoms companies, including giants such as Intel and Motorola, have long relied on manufacturing in China to sustain their business model.

Cyber security and resilience

Since the late 1990s the US has moved more decisively than any other country to defend its critical information infrastructure in cyberspace, but it also recognises that the task is extremely difficult and that major weaknesses remain. The country relies on a unique mix of assets, institutions and political foundations for its cyber civil defence.[46]

Since 2011, policy has been influenced by a deepening sense of urgency around homeland cyber defence due to espionage and attempted sabotage (with the

latter posing a threat to both infrastructure and political processes). As a result, the Trump administration encouraged a sense of national crisis in an attempt to quickly improve US national cyber preparedness. The main milestones included, in 2018, the reports 'Support to Critical Infrastructure at Greatest Risk'[47] and 'Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce';[48] National Security Presidential Memorandum 13, authorising retaliatory cyber attacks against countries engaging in systematic cyber attacks on the US;[49] and the recognition of the role of Cyber Command in homeland defence, especially in coordinating cyber missions against terrorists in US territory.[50] In May 2019 Trump issued an executive order that included a declaration by the White House of a national emergency in cyberspace.[51] And a year later, in May 2020, the US became the first country to issue a public memorandum on cyber security in space.[52]

The seriousness of the US moves was exemplified by the May 2019 executive order, which foreshadowed the termination, in certain circumstances, of all ICT trade and technology transfer between the US and China on national-security grounds. On the same day as the executive order, the Department of Commerce announced that it was adding Huawei and 68 of its non-US affiliates to the Entity List,[53] meaning that US firms and individuals would require an export licence for the sale or transfer of US technology to them.[54]

In March 2020 the Cyberspace Solarium Commission issued a report, mandated by Congress, proposing a 'strategy of layered cyber deterrence'.[55] Warning of a series of potentially devastating cyber attacks against the US, the report divided its numerous recommendations into three categories: 'Shape Behavior' (build partnerships and influence other cyberspace actors), 'Deny Benefits' (build stronger cyber defences) and 'Impose Costs' (threaten retaliation). Among the more interesting recommendations are a return to paper balloting, a public–private partnership to counteract the impact of cyber attacks, and the creation of a Bureau of Cyberspace Security and Emerging Technologies.

In November 2020 the head of CISA, Chris Krebs, was able to attest that the previous week's presidential election had been the most secure in the country's history.[56] Even though Krebs was dismissed by Trump for that statement, the achievement of a secure election was testimony to the administration's sustained efforts in this area of policy.

In summary, the US remains intensely aware of its high dependence on cyberspace and the many threats it faces, and is therefore very dissatisfied with the current state of its cyber defences. Overall, however, the US approach to national resilience and cyber security is highly sophisticated, as reflected, for example, by the International Telecommunication Union's 2018 Global Cybersecurity Index, in which it was placed second (behind the United Kingdom) out of 175 countries.[57] This assessment is unchanged by the discovery at the end of 2020 of the Russian cyber-espionage operation that had hacked into software provided by the US company SolarWinds and infected the company's many clients, including nine US government departments and about 100 private companies (investigations are ongoing). Although this will have heightened dissatisfaction with the country's cyber defences, it should also be noted that the operation was detected, and is being disrupted, by the US private sector.

Global leadership in cyberspace affairs

The US has played a leading role in improving international collaboration on cyberspace issues. One of its most focused and successful efforts led to the G8's adoption in 2003 of 11 principles for protecting critical information infrastructure.[58] One of those principles concerned the development and coordination of emergency warning systems; the sharing and analysing of information regarding vulnerabilities, threats and incidents; and the coordination of investigations into attacks on countries' infrastructure in accordance with their domestic laws. At the time, the G8 included Russia. The US was also one of the driving forces behind the adoption by a United Nations Group of Governmental Experts,[59] in 2015, of possible voluntary norms for protecting infrastructure in cyberspace – the culmination of a process that had taken more than ten years.[60]

Nevertheless, by that time, US views about the reliability of China and Russia as partners in multilateral cyberspace endeavours had hardened considerably. Quite apart from the espionage and sabotage threats that

China and Russia presented, the US was leading, or at least working with, many like-minded liberal democracies to promote their view of a free and open global internet in the face of the more authoritarian countries' desire for increased sovereign control of cyberspace. This campaign played out in many forums, but a major focus of the US effort was the perceived need to oppose the use of advanced ICT for censorship or excessive domestic surveillance. The US has concluded that the scale of the attacks being carried out against it (and key allies) by Russia and China is sufficient to render meaningful dialogue almost impossible. In fact, in 2018, in National Security Presidential Memorandum 13 (see previous section), the US shifted to a position of retaliatory attacks in cyberspace and retaliatory diplomatic measures. This has included leading more than 20 countries in publicly attributing many of the attacks.

The US occupies a position of unmatched pre-eminence in global cyberspace affairs, as demonstrated by its highly successful cyber diplomacy, the high number of leadership roles that its citizens occupy in international professional organisations such as the Institute of Electrical and Electronics Engineers (IEEE) and ISACA,[61] and its presence alongside allied countries in technical-standards groups.[62]

US offensive cyber capabilities are more developed than those of any other country

Offensive cyber capability

The US has been prepared to disclose some of its offensive cyber potential by publicly avowing a small number of its operations and by publicly announcing its CDI, encompassing the principles of defend forward and persistent engagement. Overall, however, the cyber arsenal and its planned uses are among the most carefully guarded state secrets.

US offensive cyber capabilities are more developed than those of any other country. All the principal foundations are in place: a high-grade cyber-intelligence capability complemented by high-grade human intelligence collection; leadership of the technologically advanced Five Eyes intelligence alliance; a powerful cyber-industrial and academic base; and mature doctrine and legal authorities, allowing for the responsible use of US capabilities in combat and in situations below the level of armed conflict.

It may be tempting to judge the US offensive cyber capability simply by the number of people in US Cyber Command, although it is difficult to identify those who are dedicated to offence rather than defence among its 6,000 military and civilian personnel. But that would be to ignore significant capabilities residing elsewhere, for example in the NSA, CIA and parts of the private sector. A focus on numbers might also cloud the point that quality is probably more important than quantity for the most sophisticated cyber operations.

Nevertheless, we judge that the US has a wide range of offensive cyber capabilities at all levels of sophistication. Significantly, as long ago as 2008, it was already capable of conducting the highly complex Stuxnet operation that involved intrusions by several discrete malware packages over several years, sustained system surveillance, and eventually the execution of an attack that caused physical damage to around 1,000 centrifuges used by Iran for uranium enrichment. The US envisages the use of such offensive capabilities in a wide range of scenarios, which may include disabling adversary strategic command-and-control systems and the navigational systems of missiles. Russia certainly assumes that the US has the capability and plans in place to do so,[63] since several senior US military sources have made public statements to that effect. We can be more certain that the US envisages the use of cyber capabilities in both high- and low-intensity conventional combat, with targeting options likely to include command-and-control assets, intelligence assets, weapons systems and platforms, and critical national infrastructure such as power grids and transport systems.

It is harder to judge how US capabilities stack up for offensive cyber operations below the threshold of war, particularly for influence-and-information operations. As Cyber Command's capabilities are overtly military, their use is carefully restricted under stringent US governmental authorities, hence their careful signalling under the strategy of defend forward and its retaliatory premise. CIA cyber operations may be more prevalent

in this space, but the fact that they are covert makes it impossible to judge their extent or effectiveness. Overall, it is likely that US cyber-enabled influence operations are far less prolific than those conducted by the Russians and Chinese, given the number of the latter that have been detected and publicly revealed. But that should not lead us to judge that the US has substantially less capability or weaker intent. We might instead conclude that the US use of its capability is more sophisticated, with less chance of detection, and that it is more controlled and responsible (or, from a different perspective, more constrained). It remains an open question whether the Russians and Chinese have gained an advantage owing to their growing peacetime operational experience in the aggressive use of offensive cyber for influence-and-information operations. It is likely that the CDI is an attempt to redress any perceived imbalance by moving the peacetime contested space from the United States' own networks to those of its adversaries.

The US has used cyber means to disrupt or destroy enemy IT systems or other capabilities in several settings in the last decade, some avowed publicly by the government – including attacks against the Islamic State (also known as ISIS or ISIL) and a Russian online group, the Internet Research Agency – and some revealed in the media (against China, Iran and North Korea). One of the more interesting pieces of media reporting was the alleged use, in 2014 and 2015, of cyber means to disable North Korean ballistic missiles prior to their launch.[64] An interesting avowal was Trump's admission that he authorised a cyber attack on Iran in 2019 in retaliation for its shooting down of a US drone.[65] The US amplifies its own offensive cyber capabilities by partnering with cyber-capable international allies, for example in the Stuxnet attack against Iran (with Israel) and in the campaign against the Islamic State in 2016 (with the UK and Australia). Through these attacks and other actions, the US has demonstrated a maturing determination and high levels of organisational coherence for sustained offensive cyber operations when it chooses to undertake them. These capabilities have not yet been demonstrated at their full potential.

Notes

1 White House, 'National Security Strategy of the United States of America', December 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

2 White House, 'National Cyber Strategy of the United States of America', September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

3 See US Department of Defense, 'Summary: Department of Defense Cyber Strategy 2018', https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

4 White House, 'Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities', 19 January 2021, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-taking-additional-steps-address-national-emergency-respect-significant-malicious-cyber-enabled-activities.

5 The term 'critical information infrastructure', in common use both in the US and internationally, refers to all the information systems underpinning critical national infrastructure.

6 United States Cyber Command, 'Beyond the Build: Delivering Outcomes through Cyberspace – The Commander's Vision and Guidance for US Cyber Command' 2015, https://nsarchive2.gwu.edu/dc.html?doc=2692135-Document-27.

7 There were significant new elements in the 2015 policy statements from the Pentagon, including recognition in 'Beyond the Build' that the cyber defences in the Department of Defense were inadequate to deal with the threats it was facing and that military units needed to be able to operate with degraded systems and a lack of cyber situational awareness (including command and control, intelligence and targeting data).

8 United States Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command', 2018, https://

www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

9 See US Department of Defense, 'Summary: Department of Defense Cyber Strategy 2018', p. 1: 'The Department must take action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests. Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia. We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict.'

10 White House, 'National Cyber Strategy of the United States of America', September 2018, p. 21.

11 White House, 'Memorandum on Renewing the National Security Council System', 4 February 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/04/memorandum-renewing-the-national-security-council-system. The Principals Committee is the 'senior interagency forum for consideration of policy issues affecting national security. … Its regular members will be the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Energy, the Secretary of Homeland Security, the Director of the Office of Management and Budget, the Representative of the United States of America to the United Nations, the Administrator of the United States Agency for International Development, and the Chief of Staff to the President. The Director of National Intelligence, the Chairman of the Joint Chiefs of Staff, and the Director of the Central Intelligence Agency shall attend in an advisory capacity. The Principal Deputy National Security Advisor, the Counsel to the President, the NSC Legal Advisor, and the National Security Advisor to the Vice President shall be invited to attend every meeting of the PC.'

12 *Ibid*. and Natasha Bertrand, 'Biden taps intelligence veteran for new White House cybersecurity role', Politico, 6 January 2021, https://www.politico.com/news/2021/01/06/biden-white-house-cybersecurity-neuberger-455508.

13 See CISA, 'National Infrastructure Advisory Council', https://www.cisa.gov/niac.

14 For further information, see the website of the ISACs National Council: https://www.nationalisacs.org.

15 For further information, see 'Assessments: Cyber Resilience Review (CRR)', Cybersecurity and Infrastructure Security Agency, https://www.us-cert.gov/resources/assessments; and United States Department of Homeland Security, 'Cyber Resilience Review', Factsheet, https://www.cisa.gov/sites/default/files/publications/Cyber-Resilience-Review-Fact-Sheet-508.pdf.

16 Office of Management and Budget, 'A Budget for America's Future: Analytical Perspectives', Washington DC, 2020, p. 265, https://www.govinfo.g.ov/content/pkg/BUDGET-2021-PER/pdf/BUDGET-2021-PER.pdf.

17 Director of National Intelligence, 'Industry Snapshot: Summary of Partner Responses to the FY 2015–2019 IC S&T Investment Landscape', 2015, p. 5, http://www.dni.gov/files/documents/atf/In-STeP%20-%20Industry%20Snapshot.pdf. This document provides valuable insight into the 'industrial' foundations of the US intelligence community.

18 National Academies of Sciences, Engineering, and Medicine, 'A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis', 2019, https://www.nap.edu/catalog/25335/a-decadal-survey-of-the-social-and-behavioral-sciences-a.

19 For example, on the high dollar value of foreign inputs into the US digital sector, the Organisation for Economic Co-operation and Development (OECD) stated that 'while the United States has the lowest share of foreign value added in domestic demand of OECD countries (12%), the sheer size of its economy means that in [dollar] terms it is by far the biggest consumer of foreign value added: 2.2 USD trillion, of which, 1.2 USD trillion (55%) comes from more digital-intensive industries'. See OECD, 'Measuring the Digital Transformation', March 2019, p. 228, https://www.oecd-ilibrary.org/sites/a87fd918-en/index.html?itemId=/content/component/a87fd918-en#:~:text=However%2C%20while%20the%20United%20States,comes%20from%20more%20digital%2Dintensive.

20 Jessica R. Nielsen, 'New Digital Economy Estimates', Bureau of Economic Analysis, August 2020, https://www.bea.gov/system/files/2020-08/New-Digital-Economy-Estimates-August-2020.pdf.

21 For a description of how the US measures the ICT sector, see Nielsen, 'New Digital Economy Estimates'.

22 See Erik Brynjolfsson and Avinash Collis, 'How Should We Measure the Digital Economy?', *Harvard Business Review*, November–December 2019, https://hbr.org/2019/11/how-should-we-measure-the-digital-economy.

23 See US Federal Reserve, 'Fedwire Funds Service Monthly Statistics', https://www.frbservices.org/resources/financial-services/wires/volume-value-stats/monthly-stats.html.

24 See Dan Schiller, *Digital Capitalism: Networking the Global Market System* (Cambridge, MA: MIT Press, 2000).

25 See, for example, G20, 'G20 Digital Economy Development and Cooperation Initiative', 8 September 2016, http://

www.g20chn.org/English/Documents/Current/201609/P020160908736971932404.pdf. The G20 definition of the digital economy, decided at its meeting in China in 2016, is 'a broad range of economic activities that includes using digitised information and knowledge as the key factor of production, and modern information networks as the important activity space'. The challenges of measuring and comparing different countries' digital economies have also been addressed in several OECD studies, such as the 2019 report 'Measuring the Digital Transformation: A Roadmap for the Future', 11 March 2019, https://www.oecd-ilibrary.org/docserver/9789264311992-en.pdf?expires=1595284992&id=id&accname=guest&checksum=DC8358091A60B496B5A6F525ECD799E6.

26 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.

27 OECD, 'Measuring the Digital Transformation', pp. 15, 30, The 25 technologies were: Control arrangements, Organic materials devices, Digital data transfer, Miscellaneous digital storage, Biological models algorithms, Wireless channel access, Traffic control for aircraft, Multiple transmissions, Synchronisation arrangements, Traffic control for vehicles, Film devices, Interactive television, VOD Network and access restrictions, Speech or voice analysis, Connection management, Other computational models, 3D objects manipulation, Electromagnetic waves reflection, Wireless communication services, Image analysis, Mathematical models algorithms, Transmission arrangements, Near-field transmission systems, Payment protocols, and Security and authentication.

28 See OECD, 'Measuring the Digital Transformation', p. 30.

29 See the assessment by StartupRanking.com: https://www.startupranking.com/countries. It defines a start-up as 'an organisation with high innovation competence and strong technological base, which has the faculty of an accelerated growth and maintains independence through time'. The IISS has not independently verified this ranking.

30 *Times Higher Education* World University Rankings, 2021, https://www.timeshighereducation.com/world-university-rankings/2021/world-ranking#!/page/0/length/25/sort_by/rank/sort_order/asc/cols/stats.

31 Data for the US comes from the OECD, and for China from Chinese sources.

32 Institute for Management Development, 'World Competitiveness Ranking 2020', https://www.imd.org/news/updates/IMD-2020-World-Competitiveness-Ranking-revealed.

33 United Nations Conference on Trade and Development, 'Digital Economy Report 2019', Geneva, p. 2, https://unctad.org/system/files/official-document/der2019_en.pdf.

34 Congressional Research Service, 'Global Research and Development Expenditures: Fact Sheet', updated 29 April 2020, p. 2, fig. 2, https://fas.org/sgp/crs/misc/R44283.pdf.

35 Xiaomin Mou, 'Artificial Intelligence: Investment Trends and Selected Industry Uses', EMCompass, International Finance Corporation, World Bank Group, September 2019, http://documents1.worldbank.org/curated/ar/617511573040599056/pdf/Artificial-Intelligence-Investment-Trends-and-Selected-Industry-Uses.pdf.

36 Stefano Baruffaldi et al., 'Identifying and measuring developments in artificial intelligence: Making the impossible possible', OECD Science, Technology and Industry Working Papers, no. 2020/05, p. 54, https://doi.org/10.1787/5f65ff7e-en.

37 MIT News, 'MIT reshapes itself to shape the future', 15 October 2018, http://news.mit.edu/2018/mit-reshapes-itself-stephen-schwarzman-college-of-computing-1015.

38 White House, 'Artificial Intelligence for the American People', https://trumpwhitehouse.archives.gov/ai.

39 White House, 'American Artificial Intelligence Initiative: Year One Annual Report', 2020, p. 5, https://www.whitehouse.gov/wp-content/uploads/2020/02/American-AI-Initiative-One-Year-Annual-Report.pdf.

40 Doug Brake, 'Submarine Cables: Critical Infrastructure for Global Communications', Information Technology & Innovation Foundation, April 2019, http://www2.itif.org/2019-submarine-cables.pdf.

41 See International Cable Protection Committee, 'Member List', https://www.iscpc.org/about-the-icpc/member-list.

42 According to a US diplomatic cable, the National Infrastructure Protection Plan 'requires compilation and annual update of a comprehensive inventory of CI/KR [critical infrastructure/key resources] that are located outside U.S. borders and whose loss could critically impact the public health, economic security, and/or national and homeland security of the United States. DHS in collaboration with State developed the Critical Foreign Dependencies Initiative (CFDI) to identify these critical U.S. foreign dependencies – foreign CI/KR that may affect systems within the U.S. directly or indirectly.' See Geoff Manaugh, 'Open Source Design 02: WikiLeaks Guide/Critical

Infrastructure', Domus, 29 June 2011, http://www.domusweb.it/en/architecture/2011/06/20/open-source-design-02-wikileaks-guide-critical-infrastructure.html.

43 Union of Concerned Scientists, 'UCS Satellite Database', updated 1 January 2021, https://www.ucsusa.org/resources/satellite-database.

44 Semiconductor Industry Association, '2020 – State of the U.S. Semiconductor Industry', 2020, p. 8, https://www.semiconductors.org/wp-content/uploads/2020/07/2020-SIA-State-of-the-Industry-Report-FINAL-1.pdf. Note that not all the columns add up to 100%, because other countries not named in the chart are also involved in the sector.

45 For a brief insight into this issue, see Saif M. Khan, 'US Semiconductor Exports to China: Current Policies and Trends', CSET Issues Brief, Georgetown University, October 2020, https://cset.georgetown.edu/wp-content/uploads/U.S.-Semiconductor-Exports-to-China-Current-Policies-and-Trends.pdf.

46 Greg Austin, 'US Policy: From Cyber Incidents to National Emergencies', in Greg Austin (ed.), *National Cyber Emergencies: The Return to Civil Defence* (Abingdon: Routledge, 2020), pp. 31–59.

47 For a summary, see Department of Homeland Security, 'Support to Critical Infrastructure at Greatest Risk ("Section 9 Report") Summary', 8 May 2018, https://www.cisa.gov/publication/support-critical-infrastructure-greatest-risk-section-9-report-summary.

48 National Institute of Standards and Technology, 'A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future', 10 May 2018, https://csrc.nist.gov/publications/detail/white-paper/2018/05/30/supporting-growth-and-sustainment-of-the-cybersecurity-workforce/final.

49 This document is classified. For a media report, see Ellen Nakashima, 'White House authorizes "offensive cyber operations" to deter foreign adversaries', *Washington Post*, 21 September 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

50 Joint Chiefs of Staff, 'Homeland Defense', Joint Publication 3-27, April 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_27.pdf.

51 White House, 'Executive Order on Securing the Information and Communications Technology and Services Supply Chain', 15 May 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain.

52 White House, 'Memorandum on Space Policy Directive-5 – Cybersecurity Principles for Space Systems', 4 September 2020, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems.

53 Under the US Export Authorization Act, the Entity List is a compilation of 'names of certain foreign persons – including businesses, research institutions, government and private organizations, individuals, and other types of legal persons – that are subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items'. See Bureau of Industry and Security, 'Entity List', https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.

54 Department of Commerce, 'Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List', 15 May 2019, https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd.

55 United States Cyberspace Solarium Commission, 'Final Report', March 2020, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

56 Chris Cillizza, 'The end of the Trump White House is *exactly* as bad as we thought it would be', CNN, 18 November 2020, https://edition.cnn.com/2020/11/18/politics/donald-trump-chris-krebs-fired/index.html.

57 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

58 Group of Eight, 'G8 Principles for Protecting Critical Information Infrastructures', May 2003, http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf.

59 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', undated, https://www.un.org/disarmament/ict-security.

60 United Nations General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/70/174, 22 July 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

61 ISACA – formerly the Information Systems Audit and Control Association, but now known only by its acronym – is dedicated to system security: see http://www.isaca.org. It has 75 chapters in the US but only one in China (and that is in Hong Kong). As for the IEEE, it is the largest professional organisation in the world, and influential in international cyberspace policy. In 2020, almost half of its 419,000 members were in the US. See https://www.ieee.org/about/at-a-glance.html.

62 For an overview, see Tim Nicholas Rühlig, 'Technical standardisation, China and the future international order: A European perspective', Heinrich Böll Foundation, Berlin, 2020, p. 22, https://eu.boell.org/sites/default/files/2020-03/HBS-Techn%20Stand-A4%20web-030320.pdf. The data on chairs of standards committees/secretariats held by citizens of different countries shows the US in a very strong position, second only to Germany: 'In absolute terms, however, China (SAC, holding 63 Secretariats) is still behind Germany (DIN, holding 132 Secretariats), the US (ANSI, 104 Secretariats), the United Kingdom (BSI, 77 Secretariats), France (AFNOR, 77 Secretariats), and Japan (JISC, 74 Secretariats). In IEC, Germany holds the most secretariat positions (36), followed by the US (26), Japan (24), France (22), United Kingdom (20), and Italy (13). China leads as many TCs and SCs in IEC as the Republic of Korea (both holding 10 secretariats).'

63 See Greg Austin and Pavel Sharikov, 'Preemption Is Victory: Aggravated Nuclear Instability of the Information Age', *Non-proliferation Review*, vol. 23, nos. 5–6, pp. 691–704.

64 See David E. Sanger and William J. Broad, 'Trump Inherits a Secret Cyberwar against North Korean Missiles', *New York Times*, 4 March 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer.

65 Ellen Nakashima, 'Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers', *Washington Post*, 23 June 2019, https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html.

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 UK has retained a world-leading cryptographic capability

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

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 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 AI sector in the UK has great strengths

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

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

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 report[23] 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-0.

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%20Wallace%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.

3. Canada

Canada is a highly digitised middle power with an advanced economy. It pursues a whole-of-society approach to cyber security that sits comfortably with its system of government and foreign policy. Its cyber policies, like those of the United States and United Kingdom, recognise a rich mix of stakeholders, and it has a relatively mature civil-sector cyber capability buttressed by appropriate laws and regulations. The Canadian government is also proactive in promoting digital transformation. A strong, and in some regards world-leading, tech economy gives Canada an advantage over many states with similarly sized economies. It relies, however, on other countries to provide most of the hardware that powers modern ICT systems. Its national resilience policy is well organised but less practised than it needs to be. Elements of its critical infrastructure are shared with the US (a common electric grid, for example). Canada is active in a multitude of diplomatic forums and in building cyber capacity in other states. Its cyber potential is enhanced by its proven ability to operate in alliance with other cyber-capable states: this gives it access to additional assets, especially those based in outer space. Canada is not a global operator in cyberspace in the same way that the US and the UK are, and offensive cyber, for which the country established a legal basis only in 2018, is the area in which it can do most to improve its overall cyber power.

Strategy and doctrine

Canada's public documents reveal that the country has prioritised a whole-of-society response to cyber security above all other cyber considerations, with the development of military and offensive capabilities therefore given less prominence in its published strategy than is the case in other cyber-capable states.

The National Security Policy of 2004 provided a comprehensive policy overview[1] and is still regarded as the guiding policy document.[2] Subsequent policy documents have focused more on individual security challenges, especially counter-terrorism, while also paying increasing attention to the security of critical infrastructure. The two pivotal cyber-focused documents were Canada's cyber-security strategies of 2010 and 2018. The 2010 strategy clearly prioritised the securing of government systems, leading to the development of technical solutions subsequently emulated by some of the country's close allies. At the time, the strategy's emphasis on fostering a closer partnership between the public and private sectors, and on initiatives aimed at the online security of Canadian citizens, was groundbreaking. Nevertheless, the strategy itself was very top-level, with little detail on the underpinning initiatives or the allocation of resources.

List of acronyms

CAF	Canadian Armed Forces
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DCIO	Defence Chief Information Officer
DND	Department of National Defence
ICT	information and communications technology

The 2018 strategy sought to address this, with about CA$500 million (US$400m) allocated to eight departments over five years (on top of existing cyber-security-related departmental budgets), covering substantive new cross-government initiatives ranging from the creation of a Canadian Centre for Cyber Security and a National Cyber Crime Coordination Unit to incentives for innovation, economic growth and the development of cyber talent. Uniquely, the 2018 strategy was itself created using a whole-of-society approach, with a wide consultation process that included the general public. Led by Public Safety Canada, implementation has appeared to be broadly on track, with further initiatives, announced in 2020, focusing on combating online child sexual exploitation and on improving the resilience of physical and digital critical national infrastructure. The strategy's implementation has been publicly reported by the government in a notably transparent way.

The Canadian Armed Forces (CAF) and the Department of National Defence (DND) rely on no fewer than 12 governmental and departmental policies to enable effective cyber security and defensive cyber operations,[3] although when it comes to the details of implementation, a paucity of documentation within the public domain limits the depth of any assessment. A 2009 Capstone Concept did establish, however, that Canada sees cyberspace as a realm of warfare, with an emphasis on using cyber operations in conjunction with other military capabilities to create integrated effects.[4]

Considerations of the operational aspects of cyber were also taking place well before the publication of the 2009 document.[5] Military cyber operations moved firmly into the public discussion in a 2017 defence policy, which set out a broad role for the military around cyber and stated that the CAF would 'ensure that new challenges in the space and cyber domains do not threaten Canadian defence and security objectives and strategic interests, including the economy'.[6]

Governance, command and control

As Canada is a parliamentary democracy in the British mould, command and control of cyber organisations rests ultimately with the prime minister, who oversees the minister of public safety and emergency preparedness, the minister of national defence and other statutory officers such as the director of the Communications Security Establishment (CSE), the director of the Canadian Security Intelligence Service (CSIS) and the commander-in-chief of the CAF. Like its close allies, Canada pursues a multi-stakeholder approach to governance of cyber-security policy and related industrial and educational policy. Other government bodies with a close involvement include the Royal Canadian Mounted Police, Industry Canada, the Treasury Board Secretariat and the Privacy Commissioner.[7]

This multi-stakeholder approach has been criticised within Canada on the grounds that it lacks a clearly defined leading authority.[8] However, Public Safety Canada claims the leadership role in coordinating civil-sector cyber policy,[9] while CSE's Cyber Centre focuses on the operational aspects of cyber security.[10] Although the lines of responsibility are intricate, CSE, CSIS and the CAF are accountable to the highest levels of government and report to, or are run by, cabinet-level government ministers. Inside Public Safety Canada there is a Director General for National Cyber Security reporting to the Senior Assistant Deputy Minister (the country's second-most senior civil servant).[11]

Historically, Canada's military cyber capabilities have tended to be defensive, and although other uses for cyber had already been envisaged in CAF/DND doctrine (the 2009 Capstone Concept, for example), it was only in 2019 that a cyber force was established in preparation for offensive cyber warfare. Employment of Canada's offensive cyber capabilities must be approved 'by the Government on a mission-by-mission basis consistent with the employment of other military assets and will be subject to the same rigour as other military uses of force',[12] and offensive cyber operations require the approval of both the minister of national defence and the minister of foreign affairs.[13]

For control of military operations, Canada has a Joint Force Cyber Component Commander. Responsibility for developing cyber capability and readiness sits with the Defence Chief Information Officer (DCIO), a civilian accountable to both the Chief of the Defence Staff and the Deputy Minister for Defence (the senior civil servant in the DND).[14] Reporting to the DCIO is a military officer at one-star level, the Director General Cyber,[15] who is charged with development of military cyber capabilities, as well as

responsibility for strategic and operational command and control, communications, computing and information.[16] The Canadian Forces Network Operations Centre defends and monitors DND networks,[17] although it is unclear which precise activities this entails as back-office networks and government data are also the responsibility of CSE and Shared Services Canada. Cyber situational awareness is provided through CSIS, CSE, Canadian Forces Intelligence Command and the Armed Forces Information Operations Group's Cyber Support Detachments. In 2019, the government launched a high-priority effort to improve integration of these diverse centres of information.[18]

Core cyber-intelligence capabilities

Canada's core cyber-intelligence capability is centred on CSE, which is civilian-led and subordinate to the minister of national defence. Internationally recognised for its technical expertise, CSE's capabilities are significantly enhanced through membership of the Five Eyes alliance. Like its equivalents in the other Five Eyes countries, CSE is responsible for both cyber intelligence and cyber security, allowing each discipline to benefit from the organisation's expertise in the other.

CSE is part of a well-developed Canadian intelligence and security community in which responsibility both for overseas human intelligence collection and for domestic security lies with the CSIS. In common with its Five Eyes partners, Canada's defence organisation has its own dedicated intelligence capabilities, under Canadian Forces Intelligence Command. In terms of geographical reach and budgets, the Canadian intelligence community as a whole operates at a lower level than those of the United States and the United Kingdom, although the reach and impact of CSE's cyber-intelligence capabilities are recognised by allies as a Canadian strong point.

Cyber empowerment and dependence

Canada enjoys a high level of digital empowerment, with an internet penetration rate above 90%.[19] Canadians use mobile phones (90% of households) far more than landlines (41%), while around one-third of households rely exclusively on wireless services.[20] Information and communications technology (ICT) is one of the fastest-growing sectors in the Canadian economy.[21]

Although Canada has restrictive policies that limit the operations of US telecommunications and internet providers within its borders, there is a very high level of cyberspace integration between the two countries. Canada is the primary beneficiary of that relationship, especially when it comes to managing its dependencies and vulnerabilities. The US is by far the leading destination for Canada's ICT exports and ranks second among the suppliers of Canada's ICT imports.[22] Just as the two countries have a common interest and joint operations in air defence, they also work closely on the protection of critical infrastructure.

The country's digital potential, but also the challenge it faces in maintaining a market edge in innovation, is illustrated by the Canadian company BlackBerry having produced an early smartphone that was popular worldwide until eventually it was superseded by Apple's iPhone. The government has taken an active role in expanding the digital economy, for example launching a national strategy for artificial intelligence (AI) in 2017.[23] Also in 2017, the government launched an innovation initiative in which certain areas with high concentrations of tech companies and universities were designated as 'superclusters' in five areas of research, including AI and digital technology.[24] Toronto is the main hub, accounting for 26% of Canada's ICT output and claiming to be the third-largest tech sector by region and the second-largest financial centre in North America.[25]

The 2019 Canadian Digital Charter recognises the need for government to work with the private sector and academia in expanding cyber expertise,[26] and the 2018 National Cyber Security Strategy aimed to increase the number of cyber firms and boost innovation.[27] Canada has four innovation clusters in the World Intellectual Property Organization's list of the top 100, which puts it on a similar footing to the UK (four) and Japan (five).[28]

In terms of AI research and exploitation, Canada has some notable achievements, for example occupying eighth position, just below Australia, in the Organisation for Economic Co-operation and Development's ranking of countries according to number of top-cited AI research papers their institutions produce.[29] However, the country's leading research institute has stated that the national AI strategy,

although the first of its kind in the world when it was launched in 2017, has since fallen behind those of most of other countries with similar programmes.[30]

The CAF has a high degree of dependence on digital systems and space-based communication. It has space capabilities of its own but is also uniquely placed by having been part of the US–Canada North American Aerospace Defense Command (NORAD) since 1957. By sharing a land border with the US, Canada also obtains unique dependability for its land-based telecommunications assets. In 2019, Canada joined with France, Germany, the UK and the US to create the Combined Force Space Component Command (CFSCC), following decades of space cooperation with those countries.[31]

Cyber security and resilience

Canada's high level of preparedness for a cyber emergency is illustrated by the wide-ranging series of plans and policies it has established, based in part on provincial and territorial organisations.[32] There is a comprehensive Cyber Security Event Management Plan that lists the stakeholders and outlines the actions required to deal with cyber-security incidents,[33] and clear reporting lines for cyber issues to be escalated to the appropriate government level and department. Industry regulators and non-state actors supplement sector-specific legislation. The Canadian Centre for Cyber Security hosts the national Computer Emergency Response Team.[34] Military systems are overseen by the CAF/DND, which also have clear procedures for reporting and escalating issues.[35] During certain cyber-security incidents or threat events, the CAF/DND can come to the aid of the government.[36]

Canada has well-developed processes to protect its critical infrastructure from cyber threats.[37] The government maintains a Canadian Critical Infrastructure Asset List, although it is not publicly available, and CSE is mandated to protect critical infrastructure if operators request assistance. Public–private collaboration is another element of Canadian resilience, with the National Cross-Sector Forum, for example, linking federal, provincial and territorial governments, critical infrastructure sectors and a Federal–Provincial–Territorial Critical Infrastructure Working Group.

The Canadian Network for Security Information Exchange aims to foster cooperation between private-sector cyber-security stakeholders (for example in the telecommunications, financial and energy sectors) and the government.[38] In all of these areas of critical infrastructure there is significant interdependence between Canada and the US[39] – a power outage on either side of the border, for example, would potentially also have an impact on the other country.[40] As early as 2004, the two countries signed a treaty for cooperation on the cyber security of critical infrastructure.[41] Cyber is a key component of the comprehensive bilateral defence cooperation that Canada maintains with the US.[42] A joint initiative by Public Safety Canada and the US Department of Homeland Security seeks to enhance collaboration on cyber-incident management by the national operations centres, establish information-sharing with the private sector on cyber security and continue cooperation on public-awareness efforts.[43]

Canada has well-developed processes to protect its critical infrastructure from cyber threats

Canada continues to suffer the same types of cyber attack as its Five Eyes partners: escalating cyber crime, cyber bullying, privacy breaches, state-based intrusions and attempts to use cyberspace for political-influence operations.[44] An annual survey covering business, government and the non-profit sector found in 2020 that the number of respondents anxious about high-level cyber threats had increased since 2019, but the number of organisations intending to increase their investments in cyber security had fallen.[45]

Overall, with the high priority Canada has given to cyber security since 2010, the renewed focus of its investments since it produced its 2018 cyber-security strategy, and the maturity of its approach to cyber resilience, Canada performs strongly in this category of the methodology. The International Telecommunication Union's 2018 Global Cybersecurity Index reflected this, placing Canada ninth out of 175 countries.[46]

Public Safety Canada has stated that coordination within the Five Eyes intelligence alliance has been 'pivotal in ensuring cyber security resilience within our respective countries' and that the 'strategic dialogue has made significant progress on cyber security issues, particularly with respect to information sharing on the threat environment, coordinated cyber incident response, and international policy coordination'.[47]

Global leadership in cyberspace affairs

Canada is active in international forums on cyberspace affairs, often seeking to shape the debate. Its 2019 National Cyber Security Action Plan outlined a broad diplomatic strategy, setting the goal of 'work[ing] to shape the international cyber security environment' in Canada's own interests through collaboration and coordination 'of strategic cybersecurity and cybercrime issues amongst stakeholders, and by advocating for an open, free and secure internet'.[48] This approach has seen the country participate in cyber-security discussions at an international level, such as in the United Nations Group of Governmental Experts on cyberspace security.[49] Canada has also run anti-crime and counter-terrorism capacity-building programmes through which it has contributed CA$15.6 million (US$12m) to cyber-security capacity-building in North and South America and Southeast Asia.[50] It is a signatory to the 2018 Paris Call for Trust and Security in Cyberspace, and has ratified the Convention on Cyber Crime.[51] In 2019, Canada oversaw the creation of the Rapid Response Mechanism, aimed at sharing information and threat analyses with other G7 countries so as to identify opportunities for coordinated responses to cyber attacks.[52]

Despite only announcing its intention to join the NATO Cooperative Cyber Defence Centre of Excellence in 2019, as a NATO member Canada has become involved in the Alliance's efforts to strengthen its cyber capabilities. In 2013, for example, Canada headed a Multinational Cyber Defence Capability Development project to improve NATO's surveillance and defensive capabilities.[53] It is also active in NATO's cryptographic team[54] and has a cyber-trained officer working on policy at NATO headquarters.

Canada has joined a US-led initiative to name and shame malicious state actors in cyberspace – part of the Cyber Deterrence Initiative.[55] Since its launch in 2018, 22 countries have participated in different joint (or synchronous) attribution statements.

Offensive cyber capability

Canada is open about its ability and willingness to use offensive cyber[56] in close adherence to international law,[57] and has possibly done so against the Islamic State (also known as ISIS or ISIL).[58] However, its offensive cyber capabilities are still nascent. While the CAF/DND have some offensive cyber capacity,[59] they rely heavily on the cyber expertise of CSE, a civilian organisation, albeit one that reports to the minister of national defence. Therefore, as in the UK, there is no clear distinction between military and civilian offensive cyber capabilities, only between how their use is authorised politically, depending on which piece of domestic or international law is engaged. Consequently, CSE and the Canadian military are considering adopting the UK's model and creating a national cyber force comprised of both military and civilian personnel.[60] This follows the passage into law in 2019 of Bill C-59 and the CSE Act, which together allow CSE to perform offensive cyber functions on behalf of the CAF/DND, operating under their legal mandate.[61] Given this clarification of the Canadian legal position, Canada has put itself in a better position to develop and use a wider set of offensive cyber capabilities. In doing so, it can draw upon the offensive cyber experience of its close partners the US, the UK and Australia, in terms of both running operations and capability development. One of the major advantages of belonging to a mature international cyber alliance such as the Five Eyes, therefore, is that it enables a country like Canada to develop and scale cyber capabilities more quickly and more efficiently than it otherwise would be able to.

Canada has joined a US-led initiative to name and shame malicious state actors in cyberspace

Notes

1 Canada Privy Council Office, 'Securing an Open Society: Canada's National Security Policy', 2004, http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.

2 See, for example, Public Safety Canada, 'Securing an Open Society: Canada's National Security Policy', 2015, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/scrng-en.aspx.

3 Public Works and Government Services Canada, 'Defensive Cyber Operations', Letter of Interest, Solicitation No. W6369-17DE25/B, 2017, p. 1, https://buyandsell.gc.ca/cds/public/2017/12/18/637ad14072ef720ed0c51146992cca46/ABES.PROD.PW__QE.B049.E26594.EBSU000.PDF.

4 Canadian Department of National Defence, 'Integrated Capstone Concept', 2009, pp. 28–30, http://publications.gc.ca/collections/collection_2012/dn-nd/D2-265-2010-eng.pdf.

5 Canadian House of Commons, 'Standing Committee on National Defence, Evidence, Tuesday 30 January 2018', https://www.ourcommons.ca/DocumentViewer/en/42-1/NDDN/meeting-77/evidence.

6 Canadian Armed Forces, 'Strong, Secure, Engaged: Canada's Defence Policy', 2017, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf.

7 Public Safety Canada, 'Cyber Security in the Canadian Federal Government', 2018, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-en.aspx.

8 The Standing Senate Committee on Banking, Trade and Commerce, 'Cyber Assault: It Should Keep You Up at Night', 2018, p. 29, https://sencanada.ca/content/sen/committee/421/BANC/Reports/BANC_Report_FINAL_e.pdf.

9 Public Safety Canada, 'National Cyber Security Action Plan 2019–2024', undated, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx.

10 Public Safety Canada, 'Speech on Canada's evolving national security architecture in a constantly changing and very difficult world', 15 January 2019, https://www.canada.ca/en/public-safety-canada/news/2019/01/speech-on-canadas-evolving-national-security-architecture-in-a-constantly-changing-and-very-difficult-world.html.

11 Government of Canada, 'Executive and Equivalent Level Organizational Charts', 9 April 2020, https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191211/002/index-en.aspx.

12 Canadian Armed Forces, 'Strong, Secure, Engaged: Canada's Defence Policy', p. 72. For more information on the CAF's cyber planning, see https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/cow-estimates-a-2019-20/joint-capabilities.html.

13 Numerous statements made during a Public Safety Committee meeting, 22 March 2018, https://openparliament.ca/committees/public-safety/42-1/101/?singlepage=1.

14 Len Bastien (Defence Chief Information Officer and Assistant Deputy Minister, Information Management, Department of National Defence) statement at the National Defence Committee, 30 January 2018, https://openparliament.ca/committees/national-defence/42-1/77/len-bastien-1/only.

15 *Ibid.*

16 Commodore Richard Feltham (Director General, Cyberspace, Department of National Defence) statement at the National Defence Committee, 30 January 2018, https://openparliament.ca/committees/national-defence/42-1/77/commodore-richard-feltham-1/only.

17 LCDR J.T.D.S. Turner, 'Royal Canadian Navy Cyber Incident Response Team', Canadian Forces College, 2016, p. 3, https://www.cfc.forces.gc.ca/259/290/318/192/turner.pdf.

18 See Government of Canada, 'Canadian Armed Forces Cyber Activities', 2019, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/cow-estimates-a-2019-20/joint-capabilities.html.

19 International Telecommunication Union, 'Core Household Indicators', June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/CoreHouseholdIndicators_Jun2019.xlsx.

20 Canadian Wireless and Telecommunications Association, 'Facts & Figures', 2019, https://www.cwta.ca/facts-figures.

21 International Trade Administration (United States), 'Canada: Country Commercial Guide', 3 August 2020, https://www.trade.gov/knowledge-product/canada-information-and-communications-technology-ict#:~:text=The%20Canadian%20ICT%20sector%20is,with%20%249.3%20billion%20in%202019.

22 *Ibid.*

23 OECD, Digital Economy Outlook 2020, Chapter 11, 'Artificial intelligence', https://www.oecd-ilibrary.org/sites/bb167041-en/1/3/11/index.html?itemId=/content/publication/bb167041-en&_csp_=509e10cb8ea8559b6f9cc53015e8814d&itemIGO=oecd&itemContentType=book#section-213.

24 The initiative was designed to foster further investment in these areas, based in part on a commitment of US$750 million

in matching grants from the government. See Government of Canada, 'About Canada's Supercluster Initiative program', 1 December 2020, https://www.ic.gc.ca/eic/site/093.nsf/eng/00016.html.

25 Toronto Global, 'Quick Facts', https://torontoglobal.ca/Discover-Toronto-region/Toronto-region-quick-facts.

26 Innovation, Science and Economic Development Canada, 'Canada's Digital Charter in Action: A Plan by Canadians, for Canadians', 2019, https://www.ic.gc.ca/eic/site/062.nsf/vwapj/Digitalcharter_Report_EN.pdf/$file/Digitalcharter_Report_EN.pdf.

27 Public Safety Canada, 'National Cyber Security Strategy – Canada's Vision for Security and Prosperity in the Digital Age', 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

28 Cornell University, INSEAD and the World Intellectual Property Organization, 'Global Innovation Index 2020: Who Will Finance Innovation?', pp. 54–6, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020.pdf.

29 OECD, 'Measuring the Digital Transformation: A Roadmap for the Future', 2019, p. 37, https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm.

30 Canadian Institute for Advanced Research, 'Building an AI World: Report on National and Regional AI Strategies Second Edition', May 2020, https://cifar.ca/wp-content/uploads/2020/10/building-an-ai-world-second-edition.pdf.

31 Cody Chiles, 'CFSCC establishment ceremony held at Vandenberg', Air Force Space Command, 2 October 2019, https://www.afspc.af.mil/News/Article-Display/Article/1983986/cfscc-establishment-ceremony-held-at-vandenberg.

32 Government of Canada, 'Emergency management organizations', Get Prepared website, https://www.getprepared.gc.ca/cnt/rsrcs/mrgnc-mgmt-rgnztns-en.aspx.

33 Government of Canada, 'Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2019', https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html.

34 Canadian Centre for Cyber Security, 'About the Cyber Centre', https://www.cyber.gc.ca/en/about-cyber-centre.

35 Public Works and Government Services Canada, 'Defensive Cyber Operations', Letter of Interest, Solicitation No. W6369-17DE25/B, 2017, pp. B1–3.

36 Government of Canada, 'Government of Canada, Cyber Security Event Management Plan (GC CSEMP) 2019'.

37 For further information, see Public Safety Canada, 'Critical Infrastructure', updated 19 August 2020, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx.

38 Government of Canada, 'National Cyber Protection', 2006, p. 2, http://publications.gc.ca/collections/Collection/Iu64-28-2005E.pdf.

39 Prime Minister of Canada, 'Joint Statement from President Donald J. Trump and Prime Minister Justin Trudeau', 13 February 2017, https://pm.gc.ca/en/news/statements/2017/02/13/joint-statement-president-donald-j-trump-and-prime-minister-justin.

40 *Ibid.*; and Murray Brewster, 'Norad asked Canada to "identify and mitigate" cyberthreats to critical civilian sites', CBC, 9 September 2019, https://www.cbc.ca/news/politics/norad-cyber-civilian-1.5273917.

41 Government of Canada, 'Agreement Between the Government of Canada and the Government of the United States of America for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security', Signed 1 June 2004, https://www.treaty-accord.gc.ca/text-texte.aspx?id=105000.

42 National Defence and the Canadian Armed Forces, 'The Canada–U.S. Defence Relationship', Backgrounder, 4 December 2014, http://www.forces.gc.ca/en/news/article.page?doc=the-canada-u-s-defence-relationship/hob7hd8s.

43 Public Safety Canada, 'Cybersecurity Action Plan between Public Safety Canada and the Department of Homeland Security', 2015, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-en.aspx.

44 Canadian Centre for Cyber Security, 'National Cyber Threat Assessment 2020', 20 November 2020, https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf.

45 Canadian Internet Registration Authority (CIRA), 'CIRA 2020 Cyber Security Report', https://www.cira.ca/cybersecurity-report-2020.

46 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 56, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

47 Amaliah Reiskind, 'Canada's Cyber Security: A Discussion with Public Safety Canada', NATO Association Canada, 22 August 2018, http://natoassociation.ca/canadas-cyber-security-a-discussion-with-public-safety-canada.

48 Public Safety Canada, 'National Cyber Security Action Plan 2019–2024'.

49 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.

50 Reiskind, 'Canada's Cyber Security: A Discussion with Public Safety Canada'.

51 Chart of signatures and ratifications of Treaty 185, Council of Europe, 2019, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=zrS8ISMY.

52 Stephanie Carvin, 'Canada and Cyber Governance: Mitigating Threats and Building Trust', in *Governing Cyberspace during a Crisis in Trust*, Centre for International Governance Innovation, 2019, p. 93, https://www.cigionline.org/sites/default/files/documents/Cyber%20Series%20Web2.pdf.

53 NATO Association Canada, 'In Pursuit of Total and Unbreachable Protection of Cyberspace, Part I: Canada, a Leader in Cyber Defence', 2018, http://natoassociation.ca/in-pursuit-of-total-and-unbreachable-protection-of-cyberspace-part-i-canada-a-leader-in-cyber-defence.

54 'Statement by Len Bastien [Defence Chief Information Officer and Assistant Deputy Minister, Information Management, Department of National Defence] at 8:45 a.m., National Defence Committee on Jan. 30th, 2018', https://openparliament.ca/committees/national-defence/42-1/77/len-bastien-1.

55 Communications Security Establishment, 'Canada and Allies Identify China as Responsible for Cyber-Compromise', 20 December 2018, https://cse-cst.gc.ca/en/media/media-2018-12-20.

56 *Ibid.*, p. 7.

57 Commodore Richard Feltham (Director General, Cyberspace, Department of National Defence) statement at the National Defence Committee, 30 January 2018; and Canadian Armed Forces, 'Strong, Secure, Engaged: Canada's Defence Policy', p. 72.

58 Cormac Mac Sweeney, 'Canada's Military Will Soon Be Able to Disrupt ISIS: Defence Minister', News 1130, 8 June 2017, https://www.citynews1130.com/2017/06/08/canadas-military-will-soon-able-disrupt-isis-defence-minister.

59 Howard Yu, 'Decentralized Cyber Forces: Cyber Functions at the Operational and Tactical Levels', Canadian Forces College, 2018, https://www.cfc.forces.gc.ca/259/290/405/305/yu.pdf.

60 Government of Canada, 'Future Force Design', 17 April 2019, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/departmental-plans/departmental-plan-2019-20-index/planned-results/future-force-design.html.

61 Government of Canada, 'Order Fixing August 1, 2019 as the Day on which Part 3 of that Act Comes into Force: SI/2019-70', *Canada Gazette*, Part II, vol. 153, no. 15, http://www.gazette.gc.ca/rp-pr/p2/2019/2019-07-24/html/si-tr70-eng.html.

4. Australia

Australia's cyber-security strategies have concentrated on national security, commercial cyber security, the industrial base for sovereign capability, workforce development and good international citizenship. The Australian Signals Directorate, the country's principal cyber-related agency, remains the most influential in national policymaking. The country is still developing its military cyber strategies and policies after setting up an Information Warfare Division in 2017. Australia can boast some research and industry credentials in the field of information and communications technology and cyber security, but these are growing from a low base. In part because of its 70-year membership of the Five Eyes intelligence alliance, Australia has more mature cyber capabilities than its modest defence and intelligence budgets might suggest. It is active in global diplomacy for cyber norms and cyber capacity-building. In 2016 it acknowledged for the first time that it possessed offensive cyber capabilities – examples of their use against the Islamic State (also known as ISIS or ISIL) were subsequently put into the public domain. Australia has actively supported the United States-led Cyber Deterrence Initiative, which aims to use cyber means to counter the malign cyber activity of other states. For Australia to become a more effective cyber power, it will need to make dramatically greater investments in cyber-related tertiary education and carve out a more viable sovereign cyber capability.

Strategy and doctrine

Australia's first Cyber Security Strategy, released in 2009,[1] was the result of a review of 'e-security' the previous year. It had two main initiatives: to create an official national Computer Emergency Response Team to complement or supersede the one that had been operating since 1994, which was based in a university;[2] and to establish a national Cyber Security Operations Centre. But the document consisted largely of rhetorical policies – laudable intentions around topics such as shared governmental and private-sector responsibility, facing the increasing threats, protecting Australian values, identity protection, expanding and upskilling the cyber workforce, and enhancing international collaboration. It did not propose significant new investments in support of its rhetorical commitments, except in the area of national security.

In April 2016 the government launched a new Cyber Security Strategy.[3] Subtitled 'Enabling Innovation, Growth and Prosperity', the plan was as much about better exploiting the economic opportunities of the information age as it was about security. The security-related themes were familiar from the existing strategy

List of acronyms

ACSC	Australian Cyber Security Centre
ADF	Australian Defence Force
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
DSCC	Defence Signals Intelligence and Cyber Command
ICT	information and communications technology
IWD	Information Warfare Division

documents of other countries, such as the United States, the United Kingdom and France: detect, deter and respond to threats in cyberspace, including through better anticipation of risks.[4] However, in comparison with previous strategies, the tone was more urgent. The document included a large number of new approaches to security, particularly around information-sharing between government and the private sector. It also acknowledged for the first time the government's use of offensive cyber capabilities to deter or respond to malicious cyber attacks.

Within 18 months, however, the planning processes for cyber strategy in the civilian sector were thrown into temporary disarray by major structural reforms that included changes to the status of the Australian Signals Directorate, the Australian Security Intelligence Organisation, the Australian Cyber Security Centre and the Attorney General's Department in order to carry through the creation of a new Department of Home Affairs, established formally in December 2017. It was modelled closely on the UK's Home Office but inspired also by the United States' creation of its Department of Homeland Security in 2002.

In 2020 Australia released an even more ambitious Cyber Security Strategy, with notably higher levels of funding and reflecting an even greater sense of urgency.[5] It adopted a much sharper tone around the threats from other countries (which were not named, even though the government had been vocal about banning Huawei from national systems since at least 2012) and highlighted the risks associated with rapidly changing technologies and even higher levels of connectivity. It was clear from this new document that cyber security had moved to the centre stage of Australian government thinking about national security.

The transition between the 2016 and 2020 cyber-security strategies was also evident in the domain of defence policy. The 2016 Defence White Paper made large-scale provision for the expansion of cyber and intelligence capabilities as part of a new strategic orientation around war in the information domain.[6] It repeated one of the fundamental planks of Australian security policy: deepening partnership with the US, especially through higher levels of military integration, inter-operability and intelligence-sharing.[7] This included cyber policy and operations. Cyber threats were identified as one of six key drivers of Australian military strategy.[8] The government assessed that the US would remain the pre-eminent global military power over the next two decades, in large part because of its scientific and industrial capability.

The military also saw organisational reform on cyber that occurred in tandem with the shake-up of the civil sector. On 30 June 2017, the Australian Defence Force (ADF) established a new Information Warfare Division (IWD), commanded at two-star level, which was subordinate to a new Joint Capabilities Group, commanded at three-star level (equivalent in rank in Australia to the chiefs of the single services).

One practical implication of the reforms was that new operational concepts and doctrines needed to be ironed out. This had less of an impact in the civil agencies but even there the changes were significant. In 2018 the government abandoned its commitment to an annual update of the 2016 cyber-security strategy and decided it was no longer fit for purpose. The policy environment had changed significantly with the escalation of threats in cyberspace, including the increasing use of the information domain by Russia and China for political interference, most notably by the Russians in the run-up to the 2016 US presidential election.

In 2020 Australia released an even more ambitious Cyber Security Strategy

Australia issued a Defence Strategic Update[9] and a Force Structure Plan[10] in July 2020, followed in August by the new Cyber Security Strategy. All three documents demonstrate heightened concern about threats in cyberspace, continuing commitment to previously announced reforms, and some acceleration of the pace of reforms and spending commitments. In the defence context, Prime Minister Scott Morrison saw new cyber-strike capabilities as an important part of a stiffened posture of credible deterrence.[11] For the first time in such military-policy documents, there was a greater and more urgent emphasis on strengthening information and cyber capabilities than on the traditional categories of land, sea and air. The two defence documents together represent a distinct evolution towards the

view that 'information underpins all effective military operations',[12] even though the government and the ADF continue to shy away from the concept of information dominance as used by the US. A new ADF military doctrine for cyberspace operations was also issued in 2020 but remains classified. It is understood to be essentially an Australian version of the US doctrine on cyberspace operations, with some changes of emphasis reflecting the country's quite different circumstances.

Governance, command and control

Major decisions on security policy are made by the National Security Committee of Cabinet, with the prime minister acting as de facto commander-in-chief of the armed forces and ultimate authority for all government decisions. This operates in parallel with a system of ministerial responsibility (including for the intelligence agencies) and statutory responsibility for the Chief of the Defence Force in military matters. The National Security Committee of Cabinet sets broad policy, such as approval of new strategies, and the operational priorities of the agencies. The Expenditure Review Committee of Cabinet approves funding plans, sometimes merely endorsing those made by the other committees because of some overlap in membership.

The main cyber-related intelligence agency, the Australian Signals Directorate (ASD), reports directly to the minister for defence, who authorises operations and sets the standards for protecting the privacy of citizens.[13] While therefore under civilian political control, there is also a de facto line of authority flowing from the Chief of the Defence Force, given that ASD includes a large number of military personnel. The personnel strength of ASD is not revealed publicly.

Within the ADF, the IWD has continued to evolve. When it was created in mid-2017, the IWD's most important element was the Joint Cyber Unit, projected to acquire about 1,000 personnel within a ten-year time frame. The ADF announced in January 2018 that the Joint Cyber Unit and a newly created Joint SIGINT Unit, alongside civilian teams from ASD, would operate under a new structure within the IWD, the Defence Signals Intelligence and Cyber Command (DSCC), headed by a one-star officer who had previously led teams in ASD.[14] The aim was to bring 'all ADF SIGINT and cyber personnel working within ASD together in a more refined command structure'.[15]

The DSCC provides a means of unifying ASD's primary responsibility for offensive cyber operations with the clearly competing need for the ADF to share control of that command function. The IWD is not the command authority within the ADF for those operations, since that falls to ASD. The IWD has a role similar to the 'raise, train and sustain' functions of the chiefs of service, who defer to combatant commanders for control of operations.[16]

ASD retains the lead role in civil-sector cyberspace policy, in large part through its subordinate agency, the Australian Cyber Security Centre (ACSC) which manages domestic affairs in this field. In that role, the ACSC and ASD report to the home affairs minister, even though ASD is accountable more directly to the prime minister and the minister for defence. ASD works with the Australian Security Intelligence Organisation (ASIO) on joint cyber operations inside Australia.

Core cyber-intelligence capabilities

ASD provides the bulk of the country's core cyber-intelligence capabilities, which are closely combined with its cyber-security and cyber-warfare functions. It has strong regional cyber expertise, with a focus on Southeast and East Asia, particularly Indonesia and China. ASD's wider intelligence reach is not so strong but is significantly enhanced through membership of the Five Eyes alliance.

ASD is part of a mature national intelligence community and works in close partnership with the domestic security agency, ASIO, and the external agency, the Australian Secret Intelligence Service, which specialises in overseas human intelligence collection and covert operations. Drawing on the example of the US, Australia created the post of Director of National Intelligence in 2018, to give the government a single source of authority for coordination of the analytical and collection work of all the intelligence agencies, as well as oversight of covert activity.

Cyber empowerment and dependence

Australia is among the world's leading countries in terms of average internet usage, per capita mobile-broadband

subscriptions and the proportion of companies that are engaged in e-commerce.[17] However, it falls outside the top ten in many other indicators of innovation, competitiveness and cyber security.

Since the turn of the century, Australia's digital economy has mostly stood still in relative terms – for example, its information industries' share of total global value added hardly increased between 2006 and 2016.[18] There is a mismatch between its innovation inputs (knowledge, research and investment), in which it ranked 13th in the world in 2020, and its innovation outputs, in which it ranked only 31st (with a particularly low position, 40th, in the specific area of knowledge outputs).[19] According to the same analysis, the country ranks among the world's top ten in terms of the expertise of its institutions and scientists, and access to venture capital, but performs much less well when it comes to the commercialisation of scientific knowledge.

This mismatch is reflected in the approach to artificial intelligence (AI). For example, Australia was in 11th position in a 2020 ranking of countries according to the number of top-cited AI research papers they produced,[20] yet it lacks the industrial capability to fully exploit this research in economic terms. A 2019 report commissioned by the government estimated that by 2030 the country will need to train at least 32,000 and perhaps as many as 161,000 workers as AI specialists if it is to realise the economic potential of its research strengths.[21] There have been efforts to address this issue – in 2019, for example, the government's main scientific research body published an AI road map and issued a call for public submissions on AI policy – but these initiatives will take many years to bear fruit.[22]

Australia boasts an increasing number of successes in the ICT sector, including in fields such as quantum computing, but research is often funded by US government agencies or US venture capital.[23] That said, the Department of Defence maintains a vigorous and highly regarded Defence Science and Technology Group, which has an active research and development (R&D) programme in cyberspace technologies.[24]

In 2018 the government set up the National Space Agency to help reverse the country's near-total dependence on foreign-owned satellites. It is funded at a modest level – A$9.8 million (US$6.8m) in 2019–20 – and operates 13 satellites.[25] In October 2019 the country joined a small space force with Canada, France, Germany, the UK and the US.

Overall, Australia has a modest capability to assess the security implications of imported technologies, with the best capabilities concentrated largely in government and in several larger corporations. The country contributes significantly to collaborative research both in the commercial and open-source scientific sectors, and in classified work with its closest intelligence and military allies.

Cyber security and resilience

Successive Australian governments have made important efforts to improve national cyber security and the resilience of the country's critical infrastructure.[26] An education campaign was launched in 2011 around the 'top four' threats to cyber security,[27] based on a list of mitigation strategies advocated by ASD. The four became an 'essential eight' mitigation strategies in 2017, and ASD's full list of 35 strategies was augmented to 38. The programme has been emulated in the UK and Canada. By 2020 the government had significantly improved its cyber-security guidance for all sectors.[28]

Since the turn of the century, Australia's digital economy has mostly stood still in relative terms

The state of Australia's national cyber security has been well documented in numerous government statements, several of which have found significant weaknesses in the government's own practices. The Australian National Audit Office has identified considerable recalcitrance on the part of government agencies when it comes to upgrading their cyber security – for example, its 2018 audit of three government agencies revealed that only one was compliant with the ASD top four, which were not even a particularly rigorous set of standards,[29] and in 2019 it found that the Australian postal service had not been able to manage cyber-security risks effectively.[30] In 2020, a parliamentary committee called for more reviews of

cyber security in government departments because of a continuing shortfall in compliance.[31] Nevertheless, Australia was ranked tenth out of 175 in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union (ITU).[32]

In 2016 the government created a cyber-security 'growth centre' to drive better national performance and reduce the levels of dependence on imported ICT equipment and foreign workers.[33] Now called AustCyber, it provides regular updates on the global competitiveness of the country's cyber-security sector.[34] Its 2019 update, which was notably sober in tone, reported that 'Australian demand and employment is dominated by outsourced cyber security services, and more than three-quarters of this market is controlled by foreign companies', even though these operated mostly 'from local bases and employing Australians'.[35] Such shortcomings are not surprising given that most members of the G20 – including China, France, Germany, Japan, Russia and the UK – also rely very heavily on foreign-made ICT. The document also assessed that 'several hurdles are making it difficult for Australia to fully harness existing advantages and develop a sizeable worldclass cyber security sector'.

The 2019 AustCyber update concluded that Australia needed to address its skills shortage in the cyber-security sector, do better at R&D, improve the business environment for start-ups, improve access to global markets, and develop credible metrics to assess the development of the sector and its economic impacts on the broader economy.[36] To make those steps a reality, the report urged the creation of a more advanced and resilient cyber-security mindset. If such changes are made, many in the policy community see Israel as an exemplar of what Australia could achieve.

The 2016 cyber-security strategy did not have sufficient funding to properly address the problems it identified.[37] One area that needed more attention was digital literacy, especially in tertiary (post-secondary) education – the strategy promised only A$3.5m (US$2.7m) over four years for its main initiative in that area, a programme for academic centres of excellence.[38] AustCyber reported in 2019 that the skills shortage was more severe than initially imagined.[39] By 2020 the government had realised that a cyber-security workforce of the necessary size would not be created without immigration, so it has introduced radical new visa programmes to entice workers from abroad into the field.[40] But Australian universities' response to the new opportunities and demand for cyber-security education could not match the government's ambition, particularly since the government was not prepared to invest sufficient funds. The 2020 Cyber Security Strategy invested more heavily in workforce development, education and community initiatives, providing A$50m (US$35m),[41] but this is unlikely to give universities much incentive because the government prefers community- and business-based solutions.

Many in the policy community see Israel as an exemplar of what Australia could achieve

Australia has moved towards a more coherent policy and legislative framework for cyber security and resilience, but the changes need to be reflected in better governmental coordination and more consistent use of standardised tools. The country has not yet made adequate investments to defend against the most serious potential threats.[42] Its providers of critical national infrastructure appear not to have a sufficient understanding of the risks and the situation is aggravated by a shortage of personnel with the relevant skills, including at board level.[43] However, such issues are common to all the countries studied in this report.

Global leadership in cyberspace affairs

Australia has taken an active role in the management of cyberspace issues within the framework of several international organisations, including the United Nations, ITU, Association of Southeast Asian Nations (ASEAN) and Asia-Pacific Economic Cooperation group. A prime example was its role as co-chair of a working group on cyber security in the ASEAN Plus framework. It has always cooperated closely with its allies in this regard, based on the principle laid out in its 2016 Defence White Paper that, despite having no shortage of resources, it could only deliver national security effectively by working with partners.[44] In 2017, following the example

of other countries such as the US and China, Australia published an International Cyber Engagement Strategy addressing all diplomatic aspects of cyberspace management, including cyber crime, digital trade, cyber security, human rights, privacy and international security.[45] The most innovative part of the strategy was the emerging commitment, shared with its closest allies, to undertake active defence in cyberspace, involving the setting of expectations for state behaviour, practical confidence-building measures and responding to unacceptable behaviour by states.[46] Australia has also participated in the UN Group of Governmental Experts on cyberspace security, including by chairing it from 2013–15.[47]

Australia has been implementing a modest programme of capacity-building for cyber security in Southeast Asia and the South Pacific since 2016. This has probably achieved the greatest impact in partnership with other donor governments, rather than in the projects delivered solely by Australian providers, but the effectiveness of some aspects of the programme is open to question. It is arguably unrealistic to aim to build cyber-security capacity in states with very low levels of economic development in the ICT sector, scarce resources for education and only very few officials in cyberspace-related roles. Countries as poor as Cambodia or Laos, or the microstates of the South Pacific, are less likely to profit from such projects than Indonesia or Vietnam.

The country has aligned more closely than most other US allies with Washington's move to exclude the Chinese company Huawei from national 5G networks, and was in the vanguard of international lobbying to that effect.[48] In August 2018 it became the first Five Eyes member to advise its telecoms operators to avoid purchasing 5G equipment or services from Huawei. This not only soured relations with China but also put Australia at odds with the UK and Canada on the issue for almost two years. The extent to which the decision was the outcome of broader geopolitical concerns, rather than specific technical issues, remains unclear.

Australia has been opposed to China's increasing investment in the ICT sectors of regional countries, especially in the South Pacific – a position demonstrated most strikingly in 2018 when it successfully pressured the Solomon Islands to abandon a deal with Huawei for an undersea cable to Australia in favour of a deal that excluded all Chinese companies.[49] It has not had similar success with Papua New Guinea, which is reliant on Australian aid but determined to resist pressure to abandon Huawei.[50]

The country conducts bilateral and multilateral dialogues on cyberspace affairs, including with Canada, China, India, Indonesia, Japan, New Zealand, South Korea, the UK and the US. The US–Japan–Australia trilateral dialogue is particularly important as a way for Canberra to signal its positions on internet freedom and malign behaviour by states.

Offensive cyber capability

In 2016 Australia officially avowed that it possessed an offensive cyber capability and had used it against the Islamic State (also known as ISIS or ISIL).[51] The head of ASD confirmed in 2019 that those operations had been conducted jointly with coalition partners and that the Australian dimension, under the direction of the ADF's Chief of Joint Operations, involved both the degrading of Islamic State battlefield communications and an online influence operation.[52] He added that the country's capabilities would also be directed at 'organised offshore cyber criminals'.[53] Australia has also provided support to the US Cyber Deterrence Initiative, which involves public attribution of foreign attacks and engagement in cyberspace to disrupt them. Australian offensive cyber operations are conducted in accordance with the country's understanding of international law and are closely scrutinised by a growing number of government lawyers specialising in the field.

In its five-year corporate plan published in 2019, ASD reiterated its mission on offensive cyber operations, linking it to domestic requirements (countering cyber crime) as well as to warfighting needs.[54] The plan aimed to build a world-class offensive cyber capability[55] while emphasising that ASD's ability to conduct operations would be underpinned by its close international partnerships.[56]

Overall, Australia has effective offensive cyber capabilities. Its close partnership and joint operations with the US and the UK secure its place in the front rank of states in terms of offensive cyber, while its membership of the Five Eyes alliance provides it with the enhanced intelligence and situational awareness needed for

top-end operations. At the same time, in terms of resources and available personnel, Australia does not match the capabilities of its senior allies.

In common with all other states, the biggest constraint on Australia's offensive cyber capability may well be the limited extent of its national skills base and pipeline. ASD official documents regularly allude to this challenge, and many of its public statements, including revelations of offensive cyber operations, are accompanied by recruitment appeals.

Notes

1 Australian Government, Attorney-General's Department, 'Cyber Security Strategy', Canberra, November 2009, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf.

2 See Gary Waters, 'National Cyber Emergency Policy for Australia: Critical Infrastructure', in Greg Austin (ed.), *National Cyber Emergencies: The Return to Civil Defence* (Abingdon: Routledge, 2020), pp. 93–105.

3 Australian Government, Department of the Prime Minister and Cabinet, 'Australia's Cyber Security Strategy: Enabling Innovation, Growth and Prosperity', Canberra, 2016, https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf.

4 *Ibid*., p. 6.

5 Australian Government, Department of Home Affairs, 'Australia's Cyber Security Strategy', Canberra, August 2020, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

6 Australian Government, Department of Defence, '2016 Defence White Paper', Canberra, 2016, https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf.

7 *Ibid*., p. 35.

8 *Ibid*., p. 41.

9 Australian Government, Department of Defence, '2020 Defence Strategic Update', Canberra, July 2020, https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Defence_Strategic_Update.pdf.

10 Australian Government, Department of Defence, '2020 Force Structure Plan', Canberra, July 2020, https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Force_Structure_Plan.pdf.

11 Australian Government, Prime Minister of Australia, 'Address – Launch of the 2020 Defence Strategic Update', Canberra, 1 July 2020, https://www.pm.gov.au/media/address-launch-2020-defence-strategic-update.

12 *Ibid*., p. 36.

13 Australian Government, Australian Signals Directorate, 'Accountability', https://www.asd.gov.au/accountability.

14 Australian Government, Department of Defence, 'Defence Chief Announces New Command', Canberra, 30 January 2018, https://news.defence.gov.au/media/media-releases/defence-chief-announces-new-command.

15 *Ibid*.

16 This is explained by IWD as follows: 'IWD is developing the information warfare capabilities for the ADF to employ in all its activities, such as protecting its networks and missions systems, conducting exercises and training events, supporting the community and our region in disaster relief, stability and security operations through to full conflict and war. The capabilities IWD develops are put into operation by the ADF. Chief of Joint Operations [*sic*] is responsible for how the capabilities are used to meet the directions of the Australian Government.'

17 See International Telecommunication Union, 'Statistics', https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx; and Organisation for Economic Co-operation and Development (OECD), 'Measuring the Digital Transformation: A roadmap for the future', 11 March 2019, pp. 54, 101, 121, https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm.

18 OECD, 'Measuring the Digital Transformation: A roadmap for the future', p. 71.

19 SC Johnson College of Business Cornell University, INSEAD and the World Intellectual Property Organisation, *Global Innovation Index 2020: Who Will Finance Innovation*?, 2020, pp. xxxiv, xxxvi, 15, https://www.globalinnovationindex.org/Home.

20 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.

21 Australian Government, 'Artificial Intelligence: Solving problems, growing the economy and improving our

quality of life', 2019, p. iv, https://data61.csiro.au/~/media/D61/AI-Roadmap-assets/19-00346_DATA61_REPORT_AI-Roadmap_WEB_191111.pdf?la=en&hash=58386288921D9C21EC8C4861CDFD863F1FBCD457.

22 For an overview of Australian AI policy, see the OECD AI Observatory, https://oecd.ai/dashboards/countries/Australia.

23 See, for example, the case of quantum computing at the University of Sydney, as reported in 'Global VC Bets on Australian Quantum Computing Start-Up Q-Ctrl in Us$15m Series A', Quantaneo, 10 September 2019, https://www.quantaneo.com/Global-VC-bets-on-Australian-quantum-computing-start-up-Q-CTRL-in-US15m-Series-A_a205.html; and IARPA, 'US investing in quantum tech at Sydney University', Technology Decisions, 9 May 2016, https://www.technologydecisions.com.au/content/it-management/article/us-investing-in-quantum-tech-at-sydney-uni-672014055.

24 Australian Government, Department of Defence, 'Defence Science and Technology Group', https://www.dst.defence.gov.au/division/cyber-and-electronic-warfare-division.

25 Union of Concerned Scientists, 'UCS Satellite Database', updated 1 January 2021, https://www.ucsusa.org/resources/satellite-database.

26 See Waters, 'National Cyber Emergency Policy for Australia: Critical Infrastructure'.

27 For a discussion, see Stilgherrian, 'Australia's cyber defence "pretty ordinary" before ASD's Top Four', ZDNet, 2 June 2015, https://www.zdnet.com/article/australias-cyber-defence-pretty-ordinary-before-asds-top-four.

28 See, for example, the Australian Government Information Security Manual (ISM), which 'assists in the protection of information that is processed, stored or communicated by organisations' systems'. Australian Government, Australian Signals Directorate, 'Australian Government Information Security Manual', September 2019, https://www.cyber.gov.au/ism; Australian Government, Australian Signals Directorate, 'Strategies to Mitigate Cyber Security Incidents' (which complements the advice in the ISM), February 2017, https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents; and Australian Government, Australian Signals Directorate, 'The Essential Eight Maturity Model', 26 June 2020, https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model.

29 Australian National Audit Office, 'Cyber Resilience', Auditor General Report, no. 53 of 2017–18, 28 June 2018, https://www.anao.gov.au/work/performance-audit/cyber-resilience-2017-18.

30 Australian National Audit Office, 'Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities', Auditor General Report, no. 1 of 2019–20, 4 July 2019, https://www.anao.gov.au/work/performance-audit/cyber-resilience-government-business-enterprises-and-corporate-commonwealth-entities.

31 Joint Committee on Public Audit and Accounts, 'Report 485 Cyber Resilience', December 2020, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/CyberResilience2019-20/Report.

32 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 58, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

33 The goals of the growth-centres initiative in the designated sector are to increase collaboration and commercialisation; to improve international opportunities and market access; to enhance management and workforce skills; and to identify opportunities for regulatory reform. See Australian Government, Department of Industry, Science, Energy and Resources, 'Industry Growth Centres', https://www.industry.gov.au/strategies-for-the-future/industry-growth-centres.

34 AustCyber, 'Australia's Cyber Security Sector Competitiveness Plan–2019Update', December 2019, https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019.

35 *Ibid.*, p. 33.

36 *Ibid.*, p. 10.

37 Abbey Dorian, 'Meeting Australia's Cyber Security Challenge', Australian Institute of International Affairs, 17 October 2019, http://www.internationalaffairs.org.au/australianoutlook/meeting-australias-cyber-security-challenge.

38 Australian Government, 'Portfolio budget statements 2016–17: Budget related paper no. 1.5: Education and Training Portfolio', pp. 14, 20, https://www.dese.gov.au/download/3174/education-and-training-portfolio-budget-statements-2016-17-full-version/18354/document/pdf.

39 AustCyber, 'Cyber Security Competitiveness Plan – 2019 Update', p. 11.

40 It took Australia several years to set its immigration policies in a way that would attract higher numbers of cyber-security professionals. The government started in 2017 with the overarching Global Talent Employer Sponsored (GTES) programme, which aimed to find talent for 'highly-skilled niche positions' (without specifying cyber security) that could not be filled by Australians or through other visa programmes

such as those for short-term and medium-term skilled temporary residents. This was followed in 2018 by a scheme that focused on seven 'future-focused fields', including cyber security, but employer sponsorship was still required – the aim was to recruit 5,000 immigrants in the scheme's first year of operation. In November 2019, the government launched a new programme for skilled migration that would allow applications from individuals, not just from the sponsoring employer. See Greg Austin, 'Twelve Dilemmas of Reform in Cyber Security Education', in Greg Austin (ed.), *Cyber Security Education: Principles and Policies* (Abingdon: Routledge, 2020), pp. 208–21.

41 Australian Government, Department of Home Affairs, 'Australia's Cyber Security Strategy 2020', p. 42.

42 'Australia Needs Civil Defence against the Cyber Storm: Policy Report', Research Group on Cyber War and Peace UNSW, University of New South Wales Canberra, 31 March 2019, p. 3, https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/Policy%20Report%20Cyber%20Civil%20Defence%2031%20March%202019_1.pdf.

43 Rajiv Shah, 'Protecting critical national infrastructure in an era of IT and OT convergence', Australian Strategic Policy Institute, Policy Brief, no. 18/2019, 12 July 2019, https://www.aspi.org.au/report/protecting-critical-national-infrastructure-era-it-and-ot-convergence.

44 Australian Government, Department of Defence, '2016 Defence White Paper', Canberra, 2016, p. 45, https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf. 'While Australia is the world's twelfth largest economy and has sophisticated and growing military capabilities, Australia does not have the capacity to unilaterally protect and further our global security interests. This means we will be working with our alliance partner the United States, ASEAN countries, the North Atlantic Treaty Organisation (NATO), the United Nations and other partners to achieve our common goals in protecting and promoting a stable rules-based global order.'

45 See Australian Government, Department of Foreign Affairs and Trade, 'Australia's International Cyber Engagement Strategy', October 2017, https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australias-international-cyber-engagement-strategy.

46 *Ibid*., p. 44.

47 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.

48 See 'Australia, Huawei and 5G', IISS *Strategic Comments*, vol. 25, no. 28, October 2019, https://www.iiss.org/publications/strategic-comments/2019/australia-huawei-and-5g.

49 Rosie Perper, 'Australia snubbed Huawei and completed its undersea cable project to bring high-speed internet to Pacific Islands', Business Insider, 28 August 2019, https://www.businessinsider.com.au/australia-snubs-huawei-finishes-undersea-cables-for-pacific-islands-2019-8?r=US&IR=T.

50 Alan Burkitt-Gray, 'Australia slams Huawei for "security vulnerabilities" in PNG data centre', Capacity Media, 12 August 2020, https://www.capacitymedia.com/articles/3826128/australia-slams-huawei-for-security-vulnerabilities-in-png-data-centre.

51 Parliament of Australia, 'National Security Update on Counter Terrorism: Address to the House of Representatives, Parliament House, Canberra', 23 November 2016, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/4951827%22.

52 Australian Signals Directorate, 'Director-General ASD speech to the Lowy Institute', 27 March 2019, https://www.asd.gov.au/publications/speech-lowy-institute-speech.

53 *Ibid*.

54 On warfighting, the plan says: 'ASD supports Australian Defence Force (ADF) operations around the globe, including by providing intelligence and offensive cyber capabilities to enable the warfighter and protect ADF personnel and assets'. Australian Government, Australian Signals Directorate, 'ASD Corporate Plan 2019–20', Canberra, 2019, p. 7, https://www.asd.gov.au/sites/default/files/2019-08/ASD_Corporate_Plan_final_12.pdf. The title is a little misleading, however, as the document actually covers the period 2019–23.

55 *Ibid*., p. 8.

56 *Ibid*., p. 13.

5. France

The French government has robust strategies for security in cyberspace, supported by mature institutions and regular budget infusions. France has a wide cyber-intelligence reach but keeps its cybersecurity functions organisationally separate from its intelligence community. In terms of digitisation of its society and economy, France is not one of the leaders among the world's developed countries, though its ICT sector has clear strengths. It has shown itself to be highly capable and innovative on cyber security, advocating a whole-of-society approach. It also favours regulation as a means of addressing cyber threats, exemplified by new laws on election interference and protecting critical national infrastructure. On the international stage France has promoted multilateralism on cyber issues. Its offensive cyber capability is mature but probably lags behind those of the United States and the United Kingdom. Its desire for national autonomy on key cyber capabilities denies France the potential gain from a more integrated approach with key allies, but as a result it is less dependent on them.

Strategy and doctrine

Until 2011, France's approach to issues of cyberspace security was based on a mix of technical security needs, commercial perspectives and military interests. It has since moved more decisively towards a model that gives precedence to a unified view of national security in cyberspace. There is a striking contrast between its early strategy documents and those that have emerged since 2018.

The theme of digital security was prominent in a 2008 defence white paper that noted the challenges posed by the rapid spread of information and ideas via new technology, including in the political arena.[1] This was the first time a French public-policy document had acknowledged cyber- and information-warfare threats, and expressed determination to counter them. This intention was reflected in the creation a year later of the National Cybersecurity Agency (ANSSI)[2] under the direction of the Secretariat-General for Defence and National Security (SGDSN).[3] The first national cybersecurity strategy, published in 2011, after government ministries had been targeted in cyber attacks,[4] explicitly declared France's ambition to be a global cyber power, if only in a defensive sense. A 2013 defence white paper mandated the creation of a national doctrine for responding to major cyber threats, consisting of a coordinated defensive posture mixed with a graduated response.[5] Importantly, the 2013 white paper also contained France's official recognition of cyberspace as a military operational domain, two years after the United States had done so and three years before NATO.

List of acronyms

ANSSI	National Cybersecurity Agency
CDSN	Defence and National Security Council
DGA	General Directorate for Armaments
DGSE	General Directorate for External Security
ICT	information and communications technology
MdA	Ministry of the Armed Forces
SGDSN	Secretariat-General for Defence and National Security
SOC	Security Operations Centre

At that time, France's security environment was beginning to change as the result of a series of security shocks: the Edward Snowden leaks in 2013; jihadist terrorism between 2012 and 2016; and major data breaches including the so-called 'Macron Leaks' (the leaking of emails from Emmanuel Macron's 2017 presidential-election campaign, linked to Russian political interference in favour of the National Front candidate, Marine Le Pen).[6] These events pushed France to adopt a whole-of-society approach and to give more attention to the threat of political interference, disinformation and extremist propaganda in defining its cyber strategies and policies.

The first strong indication of a major shift in cyber policy came in January 2017, when the Ministry of the Armed Forces (MdA)[7] established a Cyber Defence Command, known as ComCyber, to coordinate military cyber operations.[8] France has had an offensive cyber doctrine since then.[9] The Strategic Review of Cyber Defence, in February 2018, represented another important turning point, with major institutional reforms announced in recognition of the gravity of the threat.[10] It clarified the organisation and integration of cyber operations among government entities, along with the national and international legal framework surrounding their use.[11] Drawing from airspace monitoring and defence, it established a standing cyber-security posture for a range of circumstances from peacetime to wartime.[12] It also marked a clear evolution away from the passive-defence model of 2008 to one of active defence, including through the development of offensive cyber capabilities, strategy and doctrine that focused on adversaries' military systems.

The departure point of the 2018 review was the fact that, despite considerable efforts, France considered that it was lagging behind the other four permanent members of the United Nations Security Council in terms of cyber defences.[13] The document stated that France would commit itself to analysing cyber threats with appropriate thoroughness and in sufficient detail.[14] It laid out new objectives for promoting stability in cyberspace, including through disincentives for those who might attack French targets. It included a new system of classification for cyber attacks, suggesting that the highest level would probably justify classification under the UN Charter as an unlawful use of force.[15] It identified three technologies essential to national cyber security: detection of attacks, encryption, and the radio and mobile-telephone network for use in a national emergency.[16]

In its very wide scope and urgent tone, the 2018 review stood out from most of the equivalent documents that other countries had published by then. Although it remains the case that France is broadly in line with the positions of the US and the United Kingdom – especially on whole-of-society coordination, national industrial imperatives and skills development – the review conveyed novel postures on a number of issues. Also of note, in September 2018 the MdA introduced a policy for the armed forces to counter disinformation.[17] This was followed by two further policies in 2019: the Ministerial Policy for Defensive Cyber Warfare[18] and Public Elements for the Military Doctrine for Offensive Cyber Warfare.[19] Presented as supporting the country's strategy of achieving cyberspace superiority, the policies foreshadowed the recruitment of 1,000 new cyber personnel and allocated €1.5 billion (US$1.8bn) to the armed forces up to 2025.[20]

In 2020 and 2021 the government announced new spending plans that reflected escalating concerns about cyber threats. The first of these provided a modest €136 million (US$161m), directed at better protection of government systems,[21] but in February 2021 the cash injection was €1bn (US$1.2bn), apparently over five years, accompanied by what was in effect a new cyber-security strategy.[22] Though published only as a 33-page press kit, it contains radical targets.[23] These are broadly in line with the overall themes of the 2018 Strategic Review of Cyber Defence but reveal a new urgency and a greater emphasis on sovereign capability and economic competitiveness in the ICT sector. In the cyber-security sector, one goal is to double the workforce from 37,000 to 75,000 over five years.[24]

France maintains a clear separation between defensive and offensive cyber operations. This means that ANSSI, the leading cyber-security agency, is dedicated exclusively to defensive operations and is not part of the intelligence community, unlike the National Security Agency (NSA) in the US or Government Communications Headquarters (GCHQ) in the UK. This distinction is important for some in France, based

on an assumption that the purposes and remit of an intelligence agency, not least its disposition towards secrecy, can interfere with some of the purposes and practices needed for civil-sector cyber security, including the need for greater transparency around cyber breaches.

Governance, command and control

The course France takes on cyber issues is set by the president, with the assistance of two bodies set up in 2018. Political decisions around the formulation of cyber-defence policy are the responsibility of the Defence and National Security Council (CDSN),[25] in which ANSSI is represented by the head of the SGDSN and ComCyber is represented by the Chief of the General Staff. Another body, the Cyber Defence Executive Committee, under the authority of the president, is tasked with high-level implementation of the decisions taken by the CDSN. The responsibility of the Cyber Defence Steering Committee, under the SGDSN, is to report once a year to the prime minister on the implementation of national cyber-security strategy.[26] In practice, meaningful decision-making on cyber security and defence begins in ministerial offices and extends up to the prime minister and the president.[27] The SGDSN then transmits the impetus of political leadership, sets the agenda and ensures the application of the measures decided.[28]

There are four channels of operational accountability: in the civil sector, through ANSSI to the prime minister; in the military, through ComCyber to the Chief of the General Staff; in the intelligence agencies, through the heads of agency to the relevant ministers; and for matters related to cyber crime, through the police, who work with prosecutors and judges.[29]

Below the head of ComCyber, each service remains responsible for its own defensive cyber operations and operates its own Security Operations Centre (SOC).[30] The Centre for the Analysis of Cyber Defence[31] is the MdA's SOC. It assesses global cyber risk so that ComCyber can then act and also advise the relevant government officials. The Centre for the Review of Information Systems Security[32] conducts penetration testing and security audits on military systems. The deployable branch of ComCyber is the 807th Signals Company, based in Rennes, whose mission in operations is to secure communications and weapons systems. ComCyber had 3,400 personnel in late 2019 and plans to reach 4,500 by 2025.[33]

As with other leading cyber powers, the efficiency of the command arrangements for French cyber operations is facilitated by high-quality technical systems, strong consensus within the relevant agencies, and political leadership that understands the value of cyber capabilities for a variety of missions.

Core cyber-intelligence capability

The focal point for the production of cyber intelligence in France is the General Directorate for External Security (DGSE).[34] But, as in the Five Eyes countries, all the French intelligence agencies have cyber capabilities and, in accordance with their specific areas of competence, cyber responsibilities. Other key agencies in the *premier cercle* of the intelligence community are the Defence Intelligence and Security Directorate,[35] the Directorate of Military Intelligence[36] and the General Directorate for Internal Security.[37]

In the cyber-security sector, one goal is to double the workforce from 37,000 to 75,000 over five years

Unlike in the Five Eyes countries, the French cyber model involves, at the national level, the strict institutional separation of offensive from defensive capabilities, and of core cyber intelligence from core cyber security. ComCyber, a military entity, takes the lead in offensive cyber operations, while cyber security is the responsibility of ANSSI. Another contrast with the Five Eyes countries is that the DGSE is an entity with overall national responsibility both for signals intelligence and for human intelligence collection. This means that the development of national cyber-intelligence capabilities is just part of the DGSE's remit: there is no French agency dedicated entirely to that role, in the way that the NSA is in the US or GCHQ in the UK. While this is just one of a number of factors that make direct comparisons problematic, the evidence suggests that France's annual investments

in core cyber-intelligence capabilities are markedly less than, for example, the UK's. Whether France's organisational integration of its human and technical capabilities and separation of cyber intelligence from cyber security have some practical advantages over the model used by its Five Eyes peers is a subject of much debate.

Overall, French cyber-intelligence capabilities seem strong on certain geographical regions, such as North Africa, but lack the global reach of the Five Eyes countries, in particular the US and the UK. Indeed, the French intelligence agencies were surprised by the sophistication of the Five Eyes capabilities revealed in the Snowden leaks. However, France's capabilities are amplified by international intelligence partnerships, including particularly close ones with some Western European states, including the UK, and with the US, as well as intelligence-sharing arrangements with some of its former colonies.

The French intelligence agencies were surprised by the sophistication of the Five Eyes capabilities revealed in the Snowden leaks

Another key contrast with the Five Eyes countries is the support that French intelligence services provide to French industry's involvement in extensive industrial espionage. One former director of the DGSE claims that, during his tenure, it devoted as much as a quarter of its resources to such activities.[38] Businesses, meanwhile, have an incentive to collaborate with the intelligence agencies because of the prospect of receiving intelligence in return. The cyber component has apparently become a key part of these industrial-espionage efforts, with targets reportedly including European multinational firms, Iranian organisations and several francophone African countries.[39]

Cyber empowerment and dependence

In terms of the digitisation of society and the economy, France is not one of the leaders among the world's developed countries. In 2020 it was ranked 15th out of the 28 members of the European Union (which still included the UK) in the EU's Digital Economy and Society Index,[40] while the ICT sector accounted for 4% of GDP,[41] comprised about 110,000 companies[42] and sustained more than 700,000 jobs.[43] In the digital economy more broadly, the banking sector is one of the strongest digital performers, with FinTech alone having created 120,000 jobs.[44] French companies are highly internationalised: web companies on average generate 39% of their turnover in international markets,[45] while 52% of FinTech start-ups operate in more than one country.[46] And France is also a major consumer of digital services: its companies spend more on information technology and cyber security than their counterparts elsewhere in Europe or in the US (and incur the lowest costs when cyber incidents occur).[47]

France's start-up and innovation environment, which has benefited from reforms initiated under President Macron, is dynamic and expanding. Station F in Paris, for example, is one of the largest start-up incubators in Europe and includes cyber-security projects supported by Thales Digital Factory and Microsoft. The main areas of expertise among cyber-security start-ups are artificial intelligence (AI), blockchain, privacy and secure collaborative tools. Almost 20% of them are ANSSI-accredited,[48] which not only certifies the reliability of their products and services but also allows them to supply the government.

France has considerable strengths in AI research and its commercialisation, ranking among the top five EU countries in that respect.[49] It ranked fifth in the world in terms of its contributions to the two most prestigious AI conferences in 2020.[50] The government announced an AI strategy in 2018, with key aims including the promotion of data-sharing between the private and public sectors; renewing the four strategic sectors of healthcare, the environment, transport, and defence and security; and establishing interdisciplinary AI research hubs with links to industry.[51] The government planned to provide funding of €1.5bn (US$1.75bn) over five years, until the end of 2022.[52]

France's internet infrastructure is becoming more resilient through the diversification of its points of presence, the increased capacity if its interconnections and its high number of international points of entry. It ranks fifth in Europe in terms of its number of interconnection points,[53] representing about 4% of the worldwide total.[54]

As for regional integration, Orange maintains a long-distance optical network (WELDON) connecting the 25 largest French cities to other European metropolitan centres such as Barcelona, Frankfurt, London and Madrid.[55] In terms of network sovereignty, it seems France's core networks rely mostly on US-made servers.[56] However, the industrial landscape seems sufficiently strong and diversified to offer avenues for a 'nationalisation' of France's core network if that were to become necessary: Thales, Atos-Bull and Orange are all Europe-leading or world-leading companies either in terms of mass or secure telecommunications. Legislation passed by the National Assembly in July 2019 means ISPs now need to obtain approval from the government before using foreign hardware.[57] As a result, the main French providers have turned their backs on Huawei. France is second only to the UK as a European landing point for transatlantic cables and is also a hub for those from Asia (through the Red Sea).

France has a policy of maintaining sovereign capabilities for its key military hardware (such as sensors, command and control, stealth technology and core networks). Thales is designing, manufacturing and deploying secure networks for the MdA and for the government as a whole.[58] The armed forces are increasingly relying on information and communications technology for their flagship platforms (next-generation frigates, and the *Rafale* F4 and *Scorpion* programmes) but hope to be able to operate successfully in environments with degraded communications, command and control.

France owns and maintains a wide range of military satellites for the purposes of secure communications, imagery and signals intelligence. It has taken a stronger stance on security aspects of outer space, which it now sees as a military domain in its own right, not merely the location of supporting infrastructure for terrestrial operations. It considers space situational awareness to be the first pillar of its strategic autonomy in space. The MdA is allocating €4.3bn (US$5.1bn) to the modernisation of all its satellites and radars, as well as to the passive and active protection of space assets.[59] In February 2021 the government announced the opening in Toulouse of a NATO Centre of Excellence for space research, intending to exploit what the government claims to be Europe's largest space ecosystem (home to France's Space Command, its Space Academy, leading international space companies, and related laboratories and research centres).[60]

Cyber security and resilience

France is in many respects the leading country in the EU for cyber-security and resilience planning. In 2020, for example, an authoritative report assessed that companies in France devoted a higher proportion of their IT spending to cyber-security measures than in any other EU country.[61] A study of cyber security in companies listed in the world's six leading stock-market indexes found the companies listed in Paris's CAC 40 to have the highest levels of maturity.[62] Nevertheless, in 2021 the government revealed its dissatisfaction with private- and public-sector responses to cyber-security threats by announcing an acceleration programme and appointing a national coordinator.[63] One of the most serious threats it identified was a fourfold increase in ransomware attacks during 2020, with local-government services among the most frequent targets.[64]

The branch of government in charge of coordinating the security of France's infrastructure is the SGDSN. Its responsibilities include implementing government policies on critical national infrastructure and choosing the companies responsible for operating it. The Defence Planning Law 2014–19 created regulatory obligations for those companies, whether public or private, in terms of the security of their networks and industrial-control systems, their threat-detection capabilities and their penetration testing. Government agencies are empowered under domestic law to audit and test the companies' cyber defences[65] and to undertake cyber operations to neutralise the source of attacks ('hack back').[66] In 2019 the government signed three-year agreements with eight leading manufacturing companies to improve their cyber security,[67] and the Financial Markets Authority published new regulations requiring digital-assets providers to have resilient information systems.[68]

In an attempt to improve public–private cooperation on cyber security, the government has announced the creation of a 'national cyber-security campus'. Its three main goals will be to double down on public awareness-raising and training; to foster the sharing of skills, tools

and data among cyber-security actors; and to build up domestic industrial capability for cyber security.[69] The head of project is the CEO of Orange Cybersecurity. ANSSI is also making progress on public–public cooperation, for example having signed partnerships with the financial, railway and civil-aviation authorities.[70] France's defensive capabilities are of a high standard. At the NATO *Locked Shields* exercise in 2019, the French team came first out of the 23 participating states.[71] In the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union, France was ranked third out of 175 countries.[72]

France's defence-procurement agency, the General Directorate for Armaments (DGA),[73] has a long-standing cyber-security department as part of its information-control (Maîtrise de l'information) branch. Tasked with protecting the information and weapons systems of the armed forces, it provides technical expertise in threat intelligence, upstream research and crisis support.[74] As part of its responsibilities it conducts vulnerability research on the armed forces' systems,[75] and since 2015 it has organised cyber war games.[76] In cyber defence, the DGA's research-and-development priorities are to produce highly resilient information systems, to find solutions that will ensure the security of weapons systems and to identify the best uses of AI in cyber operations (including offensive operations). A government-supported equity fund dedicated to defence investments, DefInvest, was set up in 2017 with an initial budget of €50m (US$59m) to support small and medium enterprises.[77]

France has established a unit within the SGDSN, the Committee against Information Manipulation,[78] to address the problem of politically motivated disinformation.[79] There have been at least two cases of significant cyber-enabled foreign interference: the hacking of TV5Monde in 2016 and the Macron Leaks in 2017. Specialists confidently attributed both incidents to Russia. Though a new law in 2018 established various mechanisms to prevent the spread of manipulated information during election campaigns, it remains to be seen how effective it will be. To raise awareness and promote good practices among allies, the MdA worked with the Atlantic Council in producing a 'post-mortem' analysis of the Macron Leaks.[80]

Global leadership in cyberspace affairs

On the international stage, France sees its responsibilities in the light of its status as one of the five permanent members of the UN Security Council and its leading positions in the EU and NATO. It seeks to maintain a form of inclusive multilateralism and to open up debates on cyberspace governance to non-state actors. Its 'International Digital Strategy' places great emphasis on promoting an 'open, diverse and trusted' cyberspace, in which it anticipates the EU can be a key player.[81] France aims to promote existing institutional mechanisms in order to 'limit hacking and destabilising activities' in cyberspace, notably through an international initiative, the 'Paris Call for Trust and Security in Cyberspace',[82] unveiled in November 2018. It is also actively involved in the related UN Group of Governmental Experts[83] and has been influential in the framing of the EU Cybersecurity Act. In 2019 France joined New Zealand in launching the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online, having earlier called for the creation of an appropriate regulatory framework within the EU.[84]

France pursues vigorous cyber diplomacy with key states on a bilateral level, as well as through mechanisms such as the G7. In 2020, for example, France and Germany published their third annual ICT security assessment.[85] In 2019 the third India–France cyber dialogue was held,[86] and France's presidency of the G7 saw the launch of an initiative on sharing best practices and lessons learned from the implementation of voluntary norms for cyberspace.[87] In 2018, in the Organisation for Economic Co-operation and Development, France initiated the annual Global Forum on Digital Security for Economic Prosperity, aimed at promoting the established French position that the private sector has a significant role to play in the security and stability of cyberspace.[88]

France has played a leading role in mobilising the EU's adoption of sanctions against the perpetrators of cyber attacks targeting European and national interests. In 2020 it joined the first EU sanctions against Russia and China in response to their cyber attacks,[89] which included a travel ban and asset freezes on four members of Russia's military intelligence directorate (GRU) and two Chinese nationals.[90] In its interpretation of international law,

France adopts a different position from its closest allies on the right to retaliate against cyber attacks below the threshold of armed attack, taking the view that it would be legitimate to retaliate against a series of attacks that together constitute hostile intent, even if, taken individually, none of them crosses the threshold.[91]

Offensive cyber capability

France's ComCyber has an operational complement of approximately 3,400 personnel (of which around 600 are reported to be ICT specialists), and aims to have 4,500 by 2025.[92] Its commander, General Didier Tisseyre, has stated that 40% of the personnel work on offensive operations, a share that is expected to grow in the coming years.[93]

Official and unofficial statements, as well as leaked forensic reports, have confirmed France's use of cyberspace for both disruption[94] and espionage.[95] According to General François Lecointre of the French Army, the country has also conducted cyber operations against terrorist groups in the Sahel and the Sahara.[96] Although there is little public evidence of France carrying out other destructive cyber operations, its record of robust retaliatory responses in national-security situations suggests it is prepared to do so in certain circumstances, as its leaders have acknowledged.[97] Official policy concerning offensive cyber operations places great emphasis on considering and mitigating political, legal and military risks of collateral damage to civilian infrastructure.[98] It is therefore unlikely that France would rely on private companies for offensive operations, beyond technical support.

Overall, we believe that France has a considerable offensive cyber capability. However, as in the closely related area of core cyber-intelligence capabilities, it probably lags behind the US and the UK.

Notes

1 Ministère des Armées, 'Livre blanc: Défense et sécurité nationale', 2008, http://archives.livreblancdefenseetsecurite.gouv.fr/2008/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/livre_blanc_1337/livre_blanc_1340/index.html.

2 Agence nationale de la sécurité des systèmes d'information

3 Secrétariat général de la défense et de la sécurité nationale

4 Agence nationale de la sécurité des systèmes d'information, 'Défense et sécurité des systèmes d'information: Stratégie de la France', 2011, https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.

5 Ministère des Armées, 'Livre blanc: Défense et sécurité nationale', 2013, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

6 Jean-Baptiste Jeangène Vilmer, 'The "#Macron Leaks" operation: A post-mortem', Atlantic Council, 20 June 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem.

7 Ministère des Armées

8 Ministère des Armées, 'Le commandement de la cyberdéfense (COMCYBER)', https://www.defense.gouv.fr/ema/organismes-interarmees/le-comcyber/le-comcyber/comcyber.

9 Ministère des Armées, 'Éléments publics de doctrine militaire de lutte informatique offensive', 2019, p. 4, https://www.defense.gouv.fr/fre/content/download/551497/9393997/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf. It was revealed in this 2019 document that an offensive cyber doctrine had been in place in 2017.

10 Secrétariat Général de la Défense et de la Sécurité Nationale, 'Revue stratégique de cyberdéfense', 12 February 2018, http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

11 François Delerue and Aude Gery, 'France's Cyberdefense Strategic Review and International Law', Lawfare, 23 March 2018, https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law.

12 Arthur P. Laudrain, 'French Cyber Security and Defence: Strategy, Policy-Making and Coordination', SSRN Working Paper Series, v.2.3.3, 2019, p. 20, http://dx.doi.org/10.2139/ssrn.3432338.

13 Secrétariat Général de la Défense et de la Sécurité Nationale, 'Révue stratégique de cyberdéfense', p. 7.

14 *Ibid.*, p. 135.

15 *Ibid.*, p. 80.

16 *Ibid.*, pp. 96–100.

17 Florence Parly, 'Déclaration de Mme Florence Parly, ministre des armées, sur la manipulation de l'information', Vie publique, 4 September 2018, https://www.vie-publique.fr/discours/206652-declaration-de-mme-florence-parly-ministre-des-armees-sur-la-manipulat.

18 Ministère des Armées, 'Politique ministérielle de lutte informatique défensive', 2019.

19 Ministère des Armées, 'Éléments publics de doctrine militaire de lutte informatique offensive', 2019.

20 Ministère des Armées, 'Communiqué: La France se dote d'une doctrine militaire offensive dans le cyberespace et renforce sa politique de lutte informatique défensive', 18 January 2018, https://www.defense.gouv.fr/fre/salle-de-presse/communiques/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive.

21 Agence nationale de la sécurité des systèmes d'information, 'Le Volet Cybersécurité de France Relance', September 2020, https://www.ssi.gouv.fr/agence/cybersecurite/le-volet-cybersecurite-de-france-relance.

22 'Un plan à 1 milliard d'euros pour renforcer la cybersécurité', Gouvernement.fr, 18 February 2021, https://www.gouvernement.fr/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite.

23 'Dossier de presse – Cybersécurité, faire face à la menace: la stratégie française', Gouvernement.fr, 18 February 2021, https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2021/02/210218_dp_cyber_vfinale.pdf.

24 *Ibid.*, p. 6.

25 Conseil de defense et de sécurité nationale

26 Secrétariat Général de la Défense et de la Sécurité Nationale, 'Revue stratégique de cyberdéfense'.

27 Laudrain, 'French Cyber Security and Defence', p. 24.

28 *Ibid.*

29 This was recommended in the 'Revue stratégique de cyberdéfense', p. 53, and implemented by 2019. See Institut des hautes études du ministère de l'Intérieur, 'Organisation de l'État français en gestion de crise cybernétique majeure', 2019, https://inhesj.fr/articles/organisation-de-letat-francais-en-gestion-de-crise-cybernetique-majeure.

30 Laudrain, 'French Cyber Security and Defence', p. 19.

31 Centre d'analyse de lutte informatique défensive

32 Centre d'audit de la sécurité des systèmes d'information

33 COMCYBER, 'GDA Tisseyre: "On est 3400 cybercombattants et on deviendra 4500 en 2025"', @ComcyberFR on Twitter, 12 September 2019, https://twitter.com/ComcyberFR/status/1172186486134968322.

34 Direction générale de la sécurité extérieure

35 Direction du Renseignement et de la Sécurité de la Défense

36 Direction du renseignement militaire

37 Direction générale de la sécurité intérieure

38 Isabelle Laumonier, 'Internet sous l'oeil des services de renseignement', Memoire Online, c. 2003, https://www.memoireonline.com/05/06/155/m_internet-sous-l-oeil-des-services-de-renseignement14.html.

39 'France and economic intelligence', Tarlogic, 6 November 2019, https://www.tarlogic.com/en/blog/france-and-economic-intelligence.

40 European Commission, 'EU Digital Economy and Society Index 2020', https://ec.europa.eu/digital-single-market/en/desi.

41 Eurostat, 'Percentage of the ICT Sector on GDP', https://ec.europa.eu/eurostat/web/products-datasets/-/tin00074.

42 Ministry of the Economy and Finance, 'Numérique: Chiffres clés', 14 March 2019, https://www.entreprises.gouv.fr/etudes-et-statistiques/numerique-chiffres-cles.

43 G. De Prato (ed.), *The 2018 PREDICT Key Facts Report: An Analysis of ICT R&D in the EU and Beyond*, European Commission, JRC Technical Report, 2018, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC112019/jrc112019_2018_predict_key_facts_report.pdf.

44 Ministry of the Economy and Finance, 'La Fintech, le numérique au service du secteur financier', 19 January 2018, https://www.economie.gouv.fr/entreprises/fintech-innovation-finance.

45 'La French Tech', Gouvernement.fr, https://lafrenchtech.com/en.

46 'Baromètre EY - FD', France Digitale blog, accessed 8 July 2019, http://www.francedigitale.org/barometre-ey-fd.

47 Hiscox, 'Hiscox Cyber Readiness Report 2019', https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF.

48 *Ibid.*

49 European Commission, Joint Research Centre, 'AI Watch: TES Analysis of AI Worldwide Ecosystem in 2009–2018', JRC Technical Reports, LU: European Commission, 2020, pp. 30–1, https://data.europa.eu/doi/10.2760/85212.

50 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.

51 'AI for Humanity', AI for Humanity, 29 March 2018, https://www.aiforhumanity.fr.

52 *Ibid*.

53 Arcep, 'Baromètre de l'interconnexion de données en France', 27 June 2019, https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/linterconnexion-de-donnees/barometre-de-linterconnexion-de-donnees-en-france.html.

54 Calculations based on data provided by Rowan Klöti et al., 'A Comparative Look into Public IXP Datasets', *ACM SIGCOMM Computer Communication Review*, vol. 46, no. 1, 11 January 2016, pp. 21–9, https://doi.org/10/f8bkst.

55 Orange, 'Les Réseaux d'Orange: dossier de presse', February 2019, https://www.orange.com/sirius/edossiers/pdfs/reseaux-orange-2017-fr/dp_reseaux_orange_fr_full.pdf.

56 France IX, 'France-IX's Infrastructure', https://www.franceix.net/en/technical/infrastructure.

57 Wei Shi, 'French parliament passes "Huawei Law" to govern 5G security', telecoms, 26 July 2019, https://telecoms.com/498728/french-parliament-passes-huawei-law-to-govern-5g-security.

58 'Thales Modernise Les Réseaux de Télécommunications Du Ministère de La Défense', Thales Group, accessed 9 July 2019, https://www.thalesgroup.com/fr/monde/press-release/thales-modernise-les-reseaux-de-telecommunications-du-ministere-de-la-defense; and 'Thales Assure La Sécurité de l'accès à Internet Du Réseau Interministériel de l'État', Thales Group, accessed 12 July 2019, https://www.thalesgroup.com/fr/worldwide/securite/press-release/thales-assure-la-securite-de-lacces-internet-du-reseau.

59 Arthur Laudrain, 'France's "Strategic Autonomy" Takes to Space', International Institute for Strategic Studies, Military Balance blog, 14 August 2019, https://www.iiss.org/blogs/military-balance/2019/08/france-space-strategy.

60 Ministère de l'Europe et des Affaires Étrangères, 'Defence – Establishment of the NATO space centre of excellence in Toulouse – Communiqué issued by the Ministry for the Armed Forces', 5 February 2021, https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/article/defence-establishment-of-the-nato-space-centre-of-excellence-in-toulouse.

61 European Union Agency for Cybersecurity, 'NIS Investments Report', December 2020, p. 7, https://www.enisa.europa.eu/publications/nis-investments/at_download/fullReport.

62 Wavestone, 'Top Companies Cybersecurity Index: 2020 Annual Reports', https://www.wavestone.com/app/uploads/2020/07/Wavestone-Cyberindex-top-companies-2020-EN.pdf.

63 'Dossier de presse – Cybersécurité, faire face à la menace: la stratégie française', Gouvernement.fr, p. 12.

64 *Ibid*., pp. 7–11.

65 'Loi N° 2013-1168 Du 18 Décembre 2013 Relative à La Programmation Militaire Pour Les Années 2014 à 2019 et Portant Diverses Dispositions Concernant La Défense et La Sécurité Nationale – Article 22 | Legifrance', accessed 29 March 2019, https://www.legifrance.gouv.fr/eli/loi/2013/12/18/2013-1168/jo/article_22.

66 'Code de La Défense – Article L2321-2', L2321-2 Code de la défense § (2013).

67 G20 Research Group, '2019 G20 Osaka Summit Interim Compliance Report', p. 223, http://www.g20.utoronto.ca/compliance/2019osaka-interim/08-2019-g20-compliance-interim-cyber-resilience.pdf. The companies were Airbus, ArianeGroup, Dassault Aviation, MBDA, Naval Group, Nexter, Safran and Thales.

68 *Ibid*.

69 'Un campus cybersécurite pour renforcer l'écosystème français', Gouvernement.fr, accessed 25 July 2019, https://www.gouvernement.fr/partage/11104-un-campus-cybersecurite-pour-renforcer-l-ecosysteme-francais.

70 Agence nationale de la sécurité des systèmes d'information, 'Rapports d'activités', https://www.ssi.gouv.fr/agence/missions/rapports-dactivites.

71 'France Wins Cyber Defence Exercise Locked Shields 2019', NATO CCDCOE, 12 April 2019, https://ccdcoe.org/news/2019/france-wins-cyber-defence-exercise-locked-shields-2019.

72 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.

73 Direction générale de l'armement

74 Ministère des Armées, 'Livre blanc: Défense et sécurité nationale', 2013.

75 Assemblée nationale, 'Rapport d'information de Mme Alexandra Valetta Ardisson et M. Bastien Lachaud Déposé En Application de l'article 145 Du Règlement, Par La Commission de La Défense Nationale et Des Forces Armées, En Conclusion Des Travaux d'une Mission d'information Sur La Cyberdéfense', 4 July 2018, http://www2.assemblee-nationale.fr/documents/notice/15/rap-info/i1141/#P439_94811.

76 'La DGA Développe Les Jeux de Cyberguerre à Bruz', IntelligenceOnline, 11 March 2015, https://www.intelligenceonline.fr/renseignement-d-etat/2015/03/11/la-dga-developpe-les-jeux-de-cyberguerre-a-bruz,108065256-bre.

77 BPI France, 'Definvest: Fonds d'investissement dédié aux entreprises stratégiques de la Défense', accessed 8 July 2019, https://

www.bpifrance.fr/Toutes-nos-solutions/Participation-au-capital/Fonds-d-investissement-thematiques/Definvest.

78 Comité de lutte contre la manipulation de l'information (CLMI)

79 Sénat, 'Délégation Parlementaire au Renseignement: Rapport d›activité 2019–2020', 11 June 2020, http://www.senat.fr/rap/r19-506/r19-50638.html.

80 Jeangène Vilmer, 'The "#Macron Leaks" operation: A post-mortem'.

81 Ministère de l'Europe et des Affaires Étrangères, 'Stratégie internationale de la France pour le numérique', Paris, 15 December 2017, https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-strategie-internationale-de-la-france-pour-le-numerique/#:~:text=Pr%C3%A9sent%C3%A9e%20par%20le%20ministre%20de,diplomatique%20des%20ann%C3%A9es%20%C3%A0%20venir.&text=Elle%20s'articule%20autour%20de,%3A%20gouvernance%2C%20%C3%A9conomie%2C%20s%C3%A9curit%C3%A9.

82 Arthur Laudrain, 'Avoiding A World War Web: The Paris Call for Trust and Security in Cyberspace', Lawfare, 4 December 2018, https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace.

83 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.

84 Ministère de l'Europe et des Affaires Étrangères, 'Guaranteeing Cybersecurity', undated, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy/article/guaranteeing-cybersecurity.

85 Federal Office for Information Security (Germany) and Agence Nationale de la Sécurité des Systèmes d'Information, 'Third edition of the Franco-German common situational picture', 2020, https://www.ssi.gouv.fr/uploads/2020/12/anssi-bsi-common_situational_picture_2020.pdf.

86 Ministère de l'Europe et des Affaires Étrangères, 'Indo-French Bilateral Cyber Dialogue', 20 June 2019, https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/article/indo-french-bilateral-cyber-dialogue-20-06-19.

87 Ministère de l'Europe et des Affaires Étrangères, 'G7 French presidency – Cyber Norm Initiative: Synthesis of Lessons Learned and Best Practices', 26 November 2019, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/g7-french-presidency-cyber-norm-initiative-synthesis-of-lessons-learned-and.

88 Ministère de l'Europe et des Affaires Étrangères, 'Guaranteeing Cybersecurity', undated, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy/article/guaranteeing-cybersecurity.

89 Ministère de l'Europe et des Affaires Étrangères, 'EU – Cyberattacks – Q&A from the press briefing', 30 July 2020, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/eu-cyberattacks-q-a-from-the-press-briefing-30-jul-20.

90 Lorie Maglana and Sunny Man, 'Europe: EU imposes the first ever sanctions against cyber-attacks', Global Compliance News, 21 August 2020, https://globalcompliancenews.com/eu-imposes-the-first-ever-sanctions-against-cyber-attacks-20200810.

91 Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace', 9 September 2019, https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf.

92 Ministère des Armées, 'Le COMCYBER', 4 February 2021, https://www.defense.gouv.fr/ema/organismes-interarmees/le-comcyber/le-comcyber/comcyber.

93 Laurent Lagneau, 'Environ 40% des effectifs du Commandement de la cyberdéfense sont tournés vers les actions offensives', Zone Militaire, 9 May 2020, http://www.opex360.com/2020/05/09/environ-40-des-effectifs-du-commandement-de-la-cyberdefense-sont-tournes-vers-les-actions-offensives.

94 Nathalie Guibert, 'Général Lecointre: "L'indicateur de réussite n'est pas le nombre de djihadistes tués"', *Le Monde*, 13 July 2019, https://www.lemonde.fr/international/article/2019/07/12/general-lecointre-l-indicateur-de-reussite-n-est-pas-le-nombre-de-djihadistes-tues_5488379_3210.html.

95 Martin Untersinger and Jacques Follorou, 'La France suspectée de cyberespionnage', *Le Monde*, 21 March 2014, https://www.lemonde.fr/international/article/2014/03/21/la-france-suspectee-de-cyberattaque_4387232_3210.html.

96 Simon Pascal, 'Cyberdéfense. "Nous allons accroître encore les capacités de la plaque rennaise"', Ouest-France.fr, 18

December 2020, https://www.ouest-france.fr/politique/defense/cyberdefense-nous-allons-accroitre-encore-les-capacites-de-la-plaque-rennaise-7091506.

97 Robert S. Dewar (ed.), 'National Cybersecurity and Cyberdefense Policy Snapshots: Collection 1', Center for Security Studies, 2018, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf.

98 Laudrain, 'French Cyber Security and Defence', p. 9.

6. Israel

Israel was one of the first countries to identify cyberspace as a potential threat to its national security, and started to address the issue more than 20 years ago. Initially it perceived that the main threat was of cyber attacks against its critical national infrastructure, but that perception has evolved to include attacks against other nationally significant targets. Technological and geopolitical changes have driven various organisational reforms in the way Israel's national-security system responds to cyber threats, a process culminating in 2018 with the formal establishment of the Israeli National Cyber Directorate (INCD) within the office of the prime minister. The country has also drafted a formal national cyber strategy that includes close cooperation between government, the private sector and academia, and with international partners. This cooperation, led by the INCD, has created both a vibrant cyber ecosystem and a relatively high level of preparedness and resilience within the private sector. On offensive cyber operations, little has been publicly avowed, but notable attacks that have been attributed to Israel include the use of the Stuxnet worm against Iran, between 2008 and 2010, and an attack against an Iranian port in 2020. Based on such evidence, it appears that Israel has a well-developed capacity for offensive cyber operations and is prepared to undertake them in a wide range of circumstances.

Strategy and doctrine

It was around the year 2000 when Israel identified cyberspace as an emerging domain of threat to its national security, and 2002 when the government decided to establish a dedicated agency for the protection of critical information infrastructure.[1] Cyber security became a much more explicit national-security objective in November 2010, when Prime Minister Benjamin Netanyahu ordered the formation of a special team to formulate a national strategy for placing Israel among the top five leading countries in the cyber-security field. Labelled the National Cyber Initiative, the work was led by Professor Isaac Ben Israel, head of the National Council for Research and Development, whose team comprised staff from key agencies involved with cyber security. Their main practical recommendation was the need for a new governmental cyber-security organisation that would coordinate all policy efforts in order to promote national capability in cyberspace and improve Israel's preparedness to deal with cyber threats.[2]

The first National Cyber Security Strategy, published in 2017, set out the vision that Israel would become 'a leading nation in harnessing cyberspace as an engine of economic growth, social welfare and national security'. The focus was mostly on the security aspect, where the aim was that of 'keeping cyberspace safe and … confronting the various cyber threats, in accordance

List of acronyms

IDF Israel Defense Forces
INCD Israeli National Cyber Directorate
NISA National Information Security Authority

with the country's national interests'. The strategy also declared that Israel intended to continue 'as a leader in technological innovation and as an active partner in the global processes of shaping cyberspace'.[3]

In contrast with its relative transparency on the civilian use of cyberspace, Israel has been much less forthcoming in terms of publicly available information about its military use. Indeed, it has never released a military cyber strategy. But the outlines of Israel's approach are discernible from statements by senior military officers in 2009 that depicted cyberspace as a strategic warfare and operating space, and one that particularly suited the country's need for asymmetric defences.[4] In 2012 the Israel Defense Forces (IDF) declared that the country was ready and able to use cyber weapons,[5] although the conditions under which it would do so – and the nature of the weapons themselves – remain undisclosed.

In 2015, the IDF's first publicly available defence doctrine laid out its strategic and operational response to the threats it faced, including its view on the role of cyber capabilities.[6] The doctrine described cyber defence as especially important in order to safeguard the functioning of state institutions and the armed forces.[7] The IDF's cyber capabilities were presented as enabling it to leverage intelligence, carry out networked operations in a coalition, influence adversaries' perceptions and achieve legitimacy,[8] while cyber warfare was presented as playing a part in strengthening the IDF's strategic and tactical deterrence.[9]

Governance, command and control

The formulation of cyberspace policy in Israel follows the principle of ministerial responsibility in a parliamentary democracy, where key national decisions emanate from the prime minister, other ministers and senior officials in a system of cabinet government with ministerial accountability to parliament. This is complemented by a system of multi-stakeholder consultation between government, business, academics and community groups on issues including ICT industry policy, research and development (R&D), and privacy of personal information in ICT systems. Israel's command arrangements benefit from the use of high-quality technical systems, a strong commitment to cyber operations within the relevant agencies, and a political leadership that understands the value of cyber capabilities.

By 2010, changes in Israel's perception of the cyber threat had led policymakers to the conclusion that the Israeli Security Agency (Shin Bet) could not remain the lead authority for protecting the information systems of the Israeli private sector. They decided that a more bespoke solution to coordinating national cyber-defence activities was needed.[10]

In August 2011, Prime Minister Netanyahu announced the establishment of the National Cyber Bureau (NCB), which operated under his supervision and was intended to protect critical national infrastructure against cyber attacks emanating either from other countries or terrorist groups.[11] Within a few years the government perceived a need for a separate operational authority for cyber security, so in 2016 the National Cyber Security Authority (NCSA) was established.[12] Cyber governance was further rationalised in 2018 by the merger of the NCB and the NCSA into the Israeli National Cyber Directorate (INCD), tasked with protecting Israeli cyberspace and promoting Israeli leadership in the global cyber arena.[13] The INCD deals with national cyber security and does not conduct offensive cyber operations, which are handled by Israel's military and intelligence agencies.

The proposed regulatory powers of the INCD, and the legal basis for its activities, are set out in the 2018 Cyber Security and National Cyber Directorate Bill.[14] This proposed law, introduced by Netanyahu, has sparked controversy among various civilian and defence groups in Israel. Some specialists are concerned that it would provide the prime minister with unchecked powers to dictate cyber operations, thus potentially facilitating attacks on political opponents. The unpopularity of the bill also stems from the absence of restrictions on the future collection and distribution of information by the INCD.[15]

Throughout the reorganisation process, the National Information Security Authority (NISA),[16] established in 2002 within the Shin Bet, has retained responsibility for instructing, guiding and coordinating activities between the public entities and private companies considered critical for Israel's cyber security. NISA supervises the implementation of various information-security and information-protection policies.[17]

Based on publicly available information, two main bodies within the IDF have cyber responsibilities:

1. Unit 8200, the largest unit of the Military Intelligence Directorate,[18] was entrusted with the IDF's offensive cyber capabilities in 2009 and reportedly created a special 'cyber staff' in 2011 to develop and deploy offensive cyber weapons. In around 2012, as funding and personnel for military cyber programmes increased, an Office of Capabilities and Operations was created within Unit 8200.[19]

2. The General Staff's C4I[20] and Cyber Defense Directorate is tasked with advanced technological support for IDF land, sea and air operations, including cyber-defence missions.[21]

Core cyber-intelligence capability

The Israeli intelligence architecture consists of three key agencies: the Military Intelligence Directorate (often referred to by its Hebrew abbreviation, Aman), the largest, is responsible for most aspects of air, naval, ground and signals intelligence; the Secret Intelligence Service (Mossad) is charged with Israel's foreign intelligence activities; and the Israeli Security Agency (Shin Bet) administers internal intelligence operations, including those in the Israeli-occupied territories.[22] Unsurprisingly, given the troubled and often hostile relationship between Israel and its Middle Eastern neighbours, Israel spends considerably more per capita on its intelligence services than other developed states.[23]

The development of cyber-intelligence capabilities has been a major priority during Prime Minister Netanyahu's tenure (2009–present).[24] These are mainly centred in Aman's Unit 8200.[25] Representing approximately 80% of Aman's personnel, the unit has a role similar to that of the National Security Agency (NSA) in the United States and Government Communications Headquarters in the United Kingdom, with responsibility for Israel's signals-intelligence, cyber-defensive and cyber-offensive capabilities.[26] Unit 8200 is credited with developing the Stuxnet worm used against Iran's uranium-enrichment programme between 2008 and 2010.[27]

The pressures of the Arab Spring and rapid evolution of technology led to a restructuring of Aman in the early 2010s, described by insiders as a reorientation away from traditional radio and telephone signals intelligence towards internet-based capabilities.[28] Both the Mossad and the Shin Bet make extensive use of cyber-intelligence capabilities, whether their own or those of Unit 8200. In 2019 the head of the Mossad, Yossi Cohen, identified cyber as its 'main tool' in combating terrorism,[29] and Shin Bet chief Nadav Argaman asserted in 2017 that cyber capabilities had been responsible for preventing more than 2,000 terrorist attacks.[30]

The Israeli intelligence agencies have a particularly symbiotic relationship with the country's booming digital-technology sector, with the agencies investing in innovative start-ups to develop cutting-edge cyber capability while the start-ups carve out a high-value specialisation in the global market for cyber-intelligence capability.

The Israeli intelligence agencies have a particularly symbiotic relationship with the country's booming digital-technology sector

Overall, owing to the audacity, controversy and success of their operations, Israel's intelligence services have acquired a formidable reputation. That said, and despite the regional superiority of its cyber-intelligence capabilities, Israel lacks the global intelligence reach of some other states. It compensates for this through a particularly close relationship with the US cyber-intelligence community, and also through collaboration with the UK's agencies and a few other significant partnerships (for example with France, Singapore and the United Arab Emirates).

Cyber empowerment and dependence

Over the past decade Israel has created a unique cyber ecosystem that incorporates the government, academia

and industry, based on the conception that investments in human capital and industry are necessary for maintaining high-quality cyber defences and cyber superiority over its neighbours. One of the flagship initiatives in this respect is the CyberSpark Innovation Arena in the southern city of Be'er Sheva. Established in 2014 as a joint venture on the part of the INCD, the Be'er Sheva municipal government, Ben Gurion University and industrial partners such as EMC-RSA, Lockheed Martin, IBM, Deutsche Telekom, JVP Cyber Labs and Elbit systems, CyberSpark has created a multi-stakeholder 'ecosystem' for government, academia, industry, local government and civil society to develop and test new ideas and concepts regarding cyber security.[31]

The annual survey of 500 leading cyber-security companies published in *Cybercrime Magazine* demonstrates the global competitiveness of Israel's cyber industry.[32] In 2018, with no fewer than 42 companies in the list, Israel was second only to the US (354 companies). The UK, ranked third, had only half as many companies as Israel in the list, while China had only six. In fact, the gap between Israel and first place was smaller than it appeared, given that about 40 of the 'US' companies were registered there for tax and other commercial reasons but physically located in Israel. In 2020 Israel was also in second place in the same magazine's list of 150 up-and-coming cyber-security companies.[33] A further indication of Israel's remarkable strength in this area is that in 2020 it received 37% of the global total of venture-capital funding for cyber-security companies.[34]

A distinctive feature of Israel's cyber industry is its close relationship with the IDF's Unit 8200. Within Unit 8200 there is a technology section, Unit 81, that focuses on in-house R&D of cutting-edge technology for its own personnel.[35] Many people working in Israel's cyber-security start-ups – including the founders of Palo Alto Networks, NSO and Checkpoint – had served previously in Unit 8200 as combat or technology personnel. The close collaboration between Israel's military and private sectors provides a unique technological advantage for both, with new cyber technologies tried and tested on real battlegrounds, ensuring their effectiveness and scalability before they are released on the global market.[36]

According to a 2019 report by Start-Up Nation Central and the Israel Innovation Authority, the tech sector accounted for 9.2% of the Israeli job market and offered an average salary that was roughly double the national average. However, it also reported a slowing of the rate at which multinational companies were opening R&D centres in Israel.[37]

Israel has been among the few countries where courses in cyber security can be studied at high-school level,[38] and the IDF sends officers into high schools to identify potential recruits.[39] Notable cyber-related education programmes include Magshimim, which provides after-school training for gifted young computer coders and hackers from underprivileged areas – the majority of those who complete the programme are recruited into the IDF's cyber and intelligence units.[40] In 2017 the Israeli government also established the National Center for Cyber Education, aiming to expand the talent pool that the military cyber organisations draw on.[41]

In terms of artificial intelligence (AI) research, Israel scores well. It was ranked tenth, for example, in a list of the top 50 countries according to their contributions to the two most prestigious AI conferences in 2020.[42] The IDF has deployed weapons with significant autonomy, such as the *Harpy* loitering munition and fully automated self-driving military vehicles.[43] The AI start-up scene is thriving, with no fewer than 1,150 AI-focused start-ups reported in April 2020.[44] Israeli firms have a comparative advantage in developing AI services for robotics and automation.[45] At the end of 2020 the Israel Innovation Authority announced a five-year AI programme with a planned budget of NS5 billion (US$1.55bn).[46] Although the funding is likely to be significantly reduced for budgetary and political reasons,[47] the programme outlined some initial urgent projects – developing a supercomputer, promoting R&D (especially for neuro linguistic programming), developing human resources and procuring advanced equipment for Israel's universities.

Cyber security and resilience

In a January 2020 report, Israel claimed there had been no successful cyber attacks against its critical national infrastructure in the previous 12 months,[48] but noted an increasing number of attempted attacks by Iran. An example from later in the year (April 2020) was a reportedly unsuccessful Iranian cyber attack on

Israeli water-treatment facilities, which prompted a retaliatory Israeli attack on infrastructure facilities in an Iranian port.[49] The Iranian attack prompted the head of the INCD to warn that a 'cyber winter' was coming, an allusion to increasing attacks on the country and the worsening threat environment.[50] In 2021 the Manufacturers Association of Israel assessed that additional measures were needed to stem the tide of cyber attacks, and announced a plan to establish a cyber-security headquarters – modelled on the UK's government-run National Cyber Security Centre – that would coordinate mutual support among members.[51]

Israel is a particular target of cyber attacks for geo-political and ideological reasons, but also because of its rich ICT R&D environment and its position as a leading exporter of weapons. The country's overall cyber-security situation is quite solid, resting as it does on one of the most vibrant domestic cyber-security sectors in the world, so it may be something of an anomaly that it ranked only 39th out of 175 countries in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union.[52]

The mandate of the INCD includes responsibility for all aspects of cyber defence in the civilian sphere, ranging from the formulation of policy and building technological power to operational defence in cyberspace. The INCD provides incident-handling services and guidance for civil-sector firms, especially those managing critical national infrastructure, and works to increase the resilience of civilian cyberspace.[53]

The INCD guides private companies and managers of critical national infrastructure on the implementation of new technological platforms and helps them acquire the knowledge necessary to protect their systems against cyber attacks. A system called 'Showcase', launched in 2019, connects private-sector firms with the INCD and enables them to access a comprehensive, real-time picture of the level of cyber risk that they are exposed to. This will enable the INCD to integrate capabilities and knowledge held by government agencies and private firms, and to develop metrics for rating the cyber risks they face.[54]

The INCD regularly publishes guidelines and recommendations to help Israeli private companies and citizens secure their information and reduce cyber risks. In November 2018, for example, it launched three related initiatives: the country's first national cyber-incident-response plan;[55] guidance to all businesses on how to build crisis-response teams in preparation for a cyber incident;[56] and a national cyber exercise, 'Magic Circle 2', to examine the effectiveness of its cooperation with the private sector. In 2020 the INCD issued guidelines on 'Reducing Cyber Risks for Industrial Control Systems'[57] and 'Recommendations on Using Zoom Safely'.[58]

Another important element in Israel's cyber-defence operations is the Cyber Emergency Response Team, whose responsibilities include maintaining an around-the-clock reporting mechanism between the INCD and enterprises throughout the country, whether in the private sector or governmental.[59] Its analysts include former members of IDF cyber units.

Global leadership in cyberspace affairs

In pursuit of the goal of becoming one of the world's leading cyber powers, Israel is expanding and deepening its cooperation with a range of other countries. This effort includes negotiating bilateral and multilateral agreements with friendly states, establishing closer ties with international organisations and maintaining contacts with multinational companies. The best example of Israel's strong international collaborative profile has been its participation in work on possible voluntary norms for cyberspace in the United Nations Group of Governmental Experts.[60] Israel engages regularly in international forums on such issues.[61] It has also signed a number of bilateral cyber-cooperation agreements: with Japan and India in 2018,[62] Croatia, Romania and Australia in 2019,[63] and India (again)[64] and Greece[65] in 2020.

Collaboration and knowledge-sharing with private organisations around the world is a key strand of Israel's effort to enhance its international cyber profile. In November 2018, for example, the INCD – together with the Export Institute and the Ministry of Economy and Industry – staged the 'Cyber Edge 2.0' seminar for the chief information security officers of large corporations from 14 countries.[66] Earlier that year the INCD had joined with the Hebrew University of Jerusalem, the Ministry of Economy and Industry and the Inter-American Development Bank to hold a two-week training workshop for representatives and cyber professionals from 22 Latin American countries.[67] In 2020, Israel's annual

international exhibition-style event for the private sector, Cyber Tech, attracted 18,000 participants, including representatives from some 200 companies.[68]

The INCD is not the only agency taking a leading role in international cyber cooperation. The IDF's C4I and Cyber Defense Directorate, for example, held its fourth *Cyberdome* exercise in collaboration with US Cyber Command in November 2019. The Israeli delegation was led by the commander of the Cyber Defense Brigade and included representatives from Aman, the Israeli Air Force, the Israeli Navy and the Israeli Ground Forces.[69] This is only part of the bilateral military cyber-cooperation programme with the US.

These examples show that Israel's efforts to establish itself as a leader in cyber technology and cyber security place a heavy emphasis on making tangible and practical progress on mutually important cyber issues when creating new international partnerships or maintaining existing ones.

Offensive cyber capability

Israel has not publicly provided any details about its development or use of offensive cyber capabilities, just as it has never publicly disclosed information regarding its cyber-intelligence capabilities. But various official statements have provided insights into the existence of such capabilities and Israel's approach to employing them. In June 2012, then-minister of defense Ehud Barak made the first official public reference to Israel's ability to attack in the cyber domain, and though he emphasised that it was more important to invest in defensive capabilities than offensive ones, he admitted that Israel was engaged in developing both.[70]

In fact, there had already been a significant indication of Israel's offensive capabilities through public exposure of the Stuxnet malware in 2010. Reportedly the result of collaboration between the US (the NSA) and Israel (Unit 8200), Stuxnet was designed to target the supervisory control and data acquisition (SCADA) systems of Iran's uranium-enrichment centrifuges.[71] Since then, Unit 8200 has reportedly continued to develop Israel's ability to sabotage the critical national infrastructure of potential enemies, particularly Iran.[72] For example, the Flame malware used against Iran in 2012 was reportedly also the result of collaboration between Unit 8200 and the US.[73] And in 2020, members of Unit 8200 received medals for a cyber attack reportedly aimed at sabotaging facilities in an Iranian port in retaliation for an attempt by Iran to sabotage water-treatment facilities in Israel.[74] An Israeli official stated that at the time that the retaliatory cyber attack would be the first of many.[75]

Overall, it is likely that Israel is continuing to develop highly capable offensive cyber tools commensurate with its advanced cyber-intelligence capacities, and that those offensive capabilities are amplified by close collaboration with key international partners, especially the US.

Notes

1 In 2002 the Ministerial Committee for National Security adopted Resolution B/84 on 'Responsibility for Protecting Computer Systems in Israel', which provided the basis for the creation of a steering committee charged with identifying all public and private computer systems essential to Israel's national security and therefore requiring constant protection. Some of these systems were not operated by the Israel Defense Forces but by civilian or government companies. The resolution also mandated the creation of the National Information Security Authority, the unit responsible for the protection of computerised systems within the Israeli Security Agency (Shin Bet). See Gil Baram, 'The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case', *Military and Strategic Affairs*, vol. 5, no. 1, May 2013, p. 29, https://www.inss.org.il/wp-content/uploads/systemfiles/MASA5-1Eng4_Baram.pdf.

2 A similar process is currently under way with regard to artificial intelligence, aiming to establish Israel among the top five countries in the field – see, for example, Éanna Kelly, 'Israel sets out to become the next major artificial intelligence player', Science Business, 2 July 2019, https://sciencebusiness.net/

news/israel-sets-out-become-next-major-artificial-intelligence-player; and Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel* (Cham: Springer International Publishing, 2015), pp. 47–50.

3 State of Israel, Prime Minister's Office, National Cyber Directorate, 'Israel National Cyber Security Strategy in Brief', September 2017, p. 5, https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

4 Amir Oren, 'Zeyret helheymh hhedshh shel tesh"l nemtesat bershetvet mheshebyem', *Haaretz*, 1 January 2010, http://www.haaretz.co.il/misc/1.1182490.

5 Gili Cohen and Oded Yaron, 'Barak Acknowledges Israel's Cyber Offensive for First Time', *Haaretz*, 6 June 2012, https://www.haaretz.com/barack-acknowledges-israel-s-cyber-offensive-for-first-time-1.5170714.

6 Graham Allison, 'Deterring Terror: How Israel Confronts the Next Generation of Threats – English Translation of the Official Strategy of the Israel Defense Forces', Special Report, Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2016, https://www.belfercenter.org/sites/default/files/legacy/files/IDF%20doctrine%20translation%20-%20web%20final2.pdf.

7 *Ibid*., p. 22.

8 *Ibid*., p. 38.

9 *Ibid*., p. 48.

10 Government of Israel, 'Mesper hhelth 3270', 17 December 2017, https://www.gov.il/he/Departments/policies/dec_3270_2017.

11 Baram, 'The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case', pp. 29–32.

12 Government of Israel, 'Resolution no. 2444', 15 February 2015, https://www.ictrp.org/wp-content/uploads/2019/02/Government-Resolution-No-2444-Advancing-the-National-Preparedness-for-Cyber-Security.pdf. This presented Israel's operational cyber-defence strategy for the civilian economy, calling for greater coordination of all national cyber-defence bodies and laying the foundations for the creation of the NCSA for this purpose.

13 Yigal Unna, 'National Cyber Security in Israel', *Cyber, Intelligence, and Security*, vol. 3, no. 1, May 2019, p. 170, https://www.inss.org.il/publication/national-cyber-security-in-israel.

14 Amir Cahane, 'The New Israeli Cyber Draft Bill – A Preliminary Overview', The Federmann Cyber Security Research Center – Cyber Law Program, undated, https://csrcl.huji.ac.il/news/new-israeli-cyber-law-draft-bill.

15 Yaniv Kubovich, 'Cyber Bill Would Give Netanyahu Unsupervised Powers, Experts Warn', *Haaretz*, 19 March 2019, https://www.haaretz.com/israel-news/.premium-cyber-bill-would-give-israeli-prime-minister-unsupervised-powers-experts-warn-1.7040402?v=A1C59A1E1CE4E3490E38639FFA872186.

16 NISA is known as 'Re'em' in Hebrew.

17 Lior Tabansky, 'Critical infrastructure protection against cyber threats', *Military and Strategic Affairs*, vol. 3, no. 2, November 2011, pp. 72–3, https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1326273687.pdf.

18 Israel Defense Forces, 'Military Intelligence Directorate', https://www.idf.il/en/minisites/military-intelligence-directorate.

19 Yaacov Katz, 'Security and Defense: Israel's Cyber Ambiguity', *Jerusalem Post*, 31 May 2012, http://www.jpost.com/Features/Front-Lines/Security-and-Defense-Israels-Cyber-Ambiguity; and Matthew S. Cohen, Charles D. Freilich and Gabi Siboni, 'Israel and cyber space: Unique threat and response', *International Studies Perspectives*, vol. 17, no. 3, August 2016, p. 8, https://www.researchgate.net/publication/288823312_Israel_and_Cyberspace_Unique_Threat_and_Response.

20 C4I refers to 'command, control, communications, computers and intelligence'.

21 See Israel Defense Forces, 'C4I and Cyber Defense Directorate', https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate.

22 Antonella Colonna Vilasi, 'The Israeli Intelligence Community', *Sociology Mind*, vol. 8, March 2018, pp. 114–22, https://www.scirp.org/pdf/SM_2018032915444002.pdf.

23 Richard Silverstein, 'Israeli Intelligence Budget Nearly Doubles in Past Decade Under Netanyahu', Tikun Olam, 5 May 2017, https://www.richardsilverstein.com/2017/05/05/israeli-intelligence-budget-nearly-doubles-past-decade-netanyahu.

24 Kacy Zurkus, 'Netanyahu Boasts of Israel's Cyber Intelligence', *Info Security*, 26 June 2019, https://www.infosecurity-magazine.com/news/netanyahu-boasts-of-israels-cyber-1.

25 Israel Defence Forces, 'Military Intelligence Directorate'.

26 Sean Cordey, 'The Israeli Unit 8200: An OSINT-based study', Center for Security Studies, Cyber Defense Project, December 2019, p. 8, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf.

27 Amir Mizroch, 'Rise of Computer Vision Brings Obscure Israeli Intelligence Unit Into Spotlight', *Forbes*, 28 May 2018, https://www.forbes.com/sites/startupnationcentral/2018/05/28/rise-of-computer-vision-brings-obscure-israeli-intelligence-unit-into-spotlight/#91acc643c193.

28 Amir Rapaport, 'Revolution in the Intelligence Agencies', Israel Defense, 19 April 2014, https://www.israeldefense.co.il/en/content/revolution-intelligence-agencies.

29 Jonah Jeremy Bob, 'Mossad chief Yossi Cohen: Cyber intel is main tool against terrorism', *Jerusalem Post*, 26 June 2019, https://www.jpost.com/israel-news/mossad-chief-yossi-cohen-cyber-intel-is-main-tool-against-terrorism-593617.

30 'Shin Bet head says over 2,000 terror attacks thwarted with cybertech', *Times of Israel*, 27 June 2017, https://www.timesofisrael.com/shin-bet-head-says-over-2000-attacks-thwarted-with-cybertech.

31 Deborah Housen-Couriel, 'National Cyber Security Organisation: Israel', NATO Cooperative Cyber Defence Centre of Excellence, 2017, pp. 14–15, https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf.

32 Steve Morgan, 'Cybersecurity 500 by the Numbers: Breakdown by Region', *Cybercrime Magazine*, 21 May 2018, https://cybersecurityventures.com/cybersecurity-500-by-the-numbers-breakdown-by-region.

33 In the 2020 listing of the top 150 cyber-security companies, the US had 95 companies, Israel 16, the UK eight, Russia one, and China none. See Steve Morgan, 'Hot 150 Cybersecurity Companies to Watch in 2021', *Cybercrime Magazine*, 5 January 2021, https://cybersecurityventures.com/cybersecurity-companies-list-hot-150. Although quite subjective, the list indicates the amount of attention that Israeli companies in this sector attract.

34 Israel National Cyber Directorate, 'The Israeli cyber industry continues to grow: Record fundraising in 2020', 21 January 2021, https://www.gov.il/en/departments/news/2020ind.

35 Sophie Shulman, 'Unit 81: The elite military unit that caused a big bang in the Israeli tech scene', CTech, 8 January 2021, https://www.calcalistech.com/ctech/articles/0,7340,L-3886512,00.html.

36 Thomas McMullan, 'Israel's Silent Cyberpower Is Reshaping the Middle East', *OneZero*, 16 April 2019, https://onezero.medium.com/israels-silent-cyberpower-is-reshaping-the-middle-east-af1458d16a15.

37 'High-Tech Human Capital Report 2019', Start-Up Nation Central, Israel Innovation Authority, February 2019, http://mlp.startupnationcentral.org/rs/663-SRH-472/images/Start-Up%20Nation%20Centrals%20High%20Tech%20Human%20Capital%20Report%202019.pdf. For a summary, see Lilach Baumer, 'Israel's Tech Sector Grows, but Demand Still Outstrips Supply, Says Report', Calcalist, 26 February 2019, https://www.calcalistech.com/ctech/articles/0,7340,L-3796731,00.html.

38 Gil Press, '6 Reasons Israel Became A Cybersecurity Powerhouse Leading the $82 Billion Industry', *Forbes*, 18 July 2017, https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#29c1c94b420a.

39 Cordey, 'The Israeli Unit 8200: An OSINT-based study', pp. 3, 12.

40 Isaac Kfir, 'Learning from Israel's cyber playbook', Asia and the Pacific Policy Society, 5 November 2018, https://www.policyforum.net/learning-israels-cyber-playbook.

41 Daniel Estrin, 'In Israel, teaching kids cyber skills is a national mission', *Times of Israel*, 4 February 2017, https://www.timesofisrael.com/in-israel-teaching-kids-cyber-skills-is-a-national-mission.

42 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.

43 Kirsten Gronlund, 'State of AI: Artificial Intelligence, the Military and Increasingly Autonomous Weapons', Future of Life Institute, 9 May 2019, https://futureoflife.org/2019/05/09/state-of-ai.

44 Kyle Wiggers, 'Israel Risks Falling Behind in AI Despite Growth', VentureBeat, 17 February 2020, https://venturebeat.com/2020/02/17/israel-risks-falling-behind-in-ai-despite-growth.

45 European Commission, Joint Research Centre, 'AI Watch: TES Analysis of AI Worldwide Ecosystem in 2009–2018', JRC Technical Reports, 2020, p. 29, https://data.europa.eu/doi/10.2760/85212.

46 'Israel Launches National AI Plan at Cost of 1.63 Bln USD', Xinhuanet, 23 December 2020, http://www.xinhuanet.com/english/2020-12/23/c_139613874.htm.

47 Meir Orbach, 'Israel Launches National AI Program, but Lack of Budget Threatens Its Implementation', CTECH, 22 December 2020, https://www.calcalistech.com/ctech/articles/0,7340,L-3883355,00.html.

48 Israel National Cyber Directorate, 'Zero Successful Cyber Attacks on Critical National Infrastructures', 29 January 2020, https://www.gov.il/en/departments/news/cybertech2020.

49 Israel National Cyber Directorate, 'The Israel National Cyber Directorate: Iran is a main cyber threat on [sic] the Middle East', 29 June 2019, https://www.gov.il/en/departments/news/unna_cyber_week_2019.

50 '"Cyber winter is coming," warns Israel cyber chief after attack on water systems', *Times of Israel*, 28 May 2020, https://www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-a-changing-point-in-cyber-warfare.

51 Naveen Goud, 'Israel to Build a Cybersecurity Headquarters Serving Manufacturers', Cybersecurity Insiders, 7 January 2021, https://www.cybersecurity-insiders.com/israel-to-build-a-cybersecurity-headquarters-serving-manufacturers/.

52 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 64, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

53 See Israel National Cyber Directorate, http://www.gov.il/en/departments/israel_national_cyber_directorate.

54 Uri Berkowitz, 'Hesvet hemdeynh: hekyerv at hem'erekt shetkeyn at hhebrh shelkem lemteqpet Bhesyeyber hebah', Globes, 5 May 2019, http://www.globes.co.il/news/article.aspx?did=1001284397.

55 Israel National Cyber Directorate, 'National Cyber Concept for Crisis Preparedness and Management', 6 November 2018, https://www.gov.il/BlobFolder/news/cybercrisispreparedness/en/Management%20of%20crisis%20situations%20english%20final.pdf.

56 Israel National Cyber Directorate, 'Organizational Preparedness for a Cyber Crisis: Characterization & Requirements from Crisis Management Team and IR Team', 8 November 2019, https://www.gov.il/BlobFolder/news/cybercrisisforir/en/Cyber%20crisis_575941_eng%20final%2028.11.pdf.

57 Israel National Cyber Directorate, 'Guidelines on Protecting Industrial Control Systems', 13 May 2020, https://www.gov.il/en/departments/general/icssolutions.

58 Israel National Cyber Directorate, 'Recommendations on Using Zoom Safely', 5 May 2020, https://www.gov.il/en/departments/general/zoom.

59 Israel National Cyber Directorate, 'Cyber Emergency Response Team', https://www.gov.il/en/departments/news/119en.

60 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.

61 See, for example, a speech by Deputy Attorney General Roy Schöndorf, 'Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', 8 December 2020, https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.

62 Israel National Cyber Directorate, 'Lerashevnh, heskem shet"p lheylevpey meyd' vesheytevpey mev"p bethevm hesyeyber beyn yesheral veypen', 28 November 2018, http://www.gov.il/he/departments/news/cooperationjapan; and Israel National Cyber Directorate, 'Rash memshelt yesheral, benyemyen netneyhev verash memshelt hevdev nernedrh mevdey, nepgeshev heyvem bem'even hayervh hershemy shel memshelt hevdev, vhetmev 'el shevret heskemyem beyn hemdeynevt', 15 January 2018, www.gov.il/he/departments/news/india.

63 Israel National Cyber Directorate, 'Heskem hebnevt lesheytevp p'evelh bethevm hegnet hesyeyber beyn yesheral leqrevateyh', 12 September 2019, www.gov.il/he/departments/news/cybercroatia; Israel National Cyber Directorate, 'Heskem hebnevt lesheytevp p'evelh bethevm hegnet hesyeyber beyn yesheral lervemneyh', 6 June 2019, www.gov.il/he/departments/news/israel_rumania; Israel National Cyber Directorate, 'Australian–Israeli cooperation in the field of cyber', 29 January 2019, http://www.gov.il/he/departments/news/agree_australia.

64 'India and Israel Sign Agreement to Expand Cooperation in Cyber Security', RepublicWorld.com, 16 July 2020, https://www.republicworld.com/india-news/general-news/india-and-israel-sign-agreement-to-expand-cooperation-in-cyber-security.html. This agreement with India expanded on areas of cooperation covered in the two countries' 2018 agreement.

65 Israel National Cyber Directorate, 'Joint statement on cybersecurity signed between Greece and Israel', 16 June 2020, https://www.gov.il/en/departments/news/greece.

66 Israel National Cyber Directorate, 'Semyenr beynelavemy pevrets derk lentesyegy hebrevt vemmeshelvet memdeynevt yedyedvetyevt', 18 November 2018, http://www.gov.il/he/departments/news/cyberedge.

67 Israel National Cyber Directorate, 'Shet"p bethevm hegnet hesyeyber beyn yesheral lemdeynevt ameryeqh helteyneyt vheqareybeyyem', 28 March 2018, http://www.gov.il/he/departments/news/iadb.

68 Jean-Christophe Noël, 'Israeli Cyberpower: The Unfinished Development of the Start-up Nation', French Institute of International Relations, November 2020, p. 21, https://www.ifri.org/sites/default/files/atoms/files/noel_israeli_cyberpower_2020.pdf.

69 'Israel, US Conclude Joint Cyber Defense Exercise', Israel Defense, 10 November 2019, http://www.israeldefense.co.il/en/node/40871.

70 Gili Cohen and Oded Yaron, 'Sher hebyethevn hevdh lerashevnh bep'eyelvet seyyebr hetqepyet shel yesheral', *Haaretz*, 6 June 2012, http://www.haaretz.co.il/news/politics/1.1725069.

71 David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Broadway Books, 2018), p. 25.

72 Cohen, Freilich and Siboni, 'Israel and cyber space: Unique threat and response', p. 8.

73 Tabansky and Israel, *Cybersecurity in Israel*, pp. 66–7.

74 'IDF's cyber warrior 8200 intelligence unit gets medal for "recent operations"', *Times of Israel*, 25 June 2020, https://www.timesofisrael.com/idfs-cyber-warrior-8200-intelligence-unit-gets-medal-for-recent-operations.

75 *Ibid*.

7. Japan

Japan has been among the global leaders in the commercial application of information and communications technologies since the early 1980s, but its readiness to deal with the security aspects of cyberspace is a much more recent phenomenon. Its first mature cyber-security strategy was issued in 2013, building on several earlier policies that were focused on rhetorical principles of classic information security of a narrow technical kind. Japan now has a well-developed approach to the governance of cyberspace, but this constitutes a looser set of arrangements than in countries such as the United States and the United Kingdom, particularly in terms of information-sharing by the private sector. Japan's defences in cyberspace are not especially strong, with many corporations unwilling to meet the costs of bolstering them. The country's resilience planning has been rather limited, though this intensified in the run-up to the 2020 Olympic and Paralympic Games (postponed due to COVID-19). Japan still does not have an official military cyber strategy or an official military doctrine pertaining to cyberspace, though it has made modest organisational changes in its armed forces, including the creation of some dedicated cyber units. Its offensive cyber capabilities remain underdeveloped because of the constitutional and political constraints on the country's use of force. By 2020, prompted in part by the US and Australia, Japan had shifted to a more robust cyber posture because of rising concerns about China and North Korea.

Strategy and doctrine

As its title suggests, Japan's 'First National Strategy on Information Security', in 2006, was the earliest document of its kind.[1] (At the time, many countries preferred the term 'information security' to 'cyber security'.) It did not lead to many changes in policy, however, and focused largely on narrow technical aspects of cyber security that had been topical since the mid-1990s. Several related policy documents followed.

The strategy published in 2013, the first under the title of 'Cybersecurity Strategy', was a watershed event that reflected organisational measures undertaken during the previous year.[2] In comparison with the earlier documents it had a stronger overall emphasis on national security and focused much more on cyberspace as an operational environment for politics, economics, diplomacy and global influence. It was the first Japanese government document to call for the Ministry of Defense

List of acronyms

ASEAN	Association of Southeast Asian Nations
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CSSH	Cyber Security Strategic Headquarters
DIH	Defense Intelligence Headquarters
DSI	Directorate for Signals Intelligence
ICT	information and communications technology
IoT	Internet of Things
IPv6	Internet Protocol Version 6
JSDF	Japan Self-Defense Forces
MoD	Ministry of Defense
NISC	National Center of Incident Readiness and Strategy for Cybersecurity
NTT	Nippon Telegraph and Telephone

(MoD) to defend against strategic cyber attacks by other states. Referring to cyberspace as a new domain of warfare, it outlined the creation of the first cyber-defence unit within the Japan Self-Defense Forces (JSDF) and stronger coordination between civilian and military entities in cyber defence. Furthermore, it noted the importance of norms in cyberspace and the need for a multi-stakeholder approach towards internet governance. In 2013 Japan also released a new National Security Strategy, although cyber capabilities did not feature prominently within it; the principal emphasis was on developing norms for behaviour in cyberspace and closer cooperation with like-minded countries in cyber defence.[3]

A revised Cybersecurity Strategy was issued in 2015, calling for uniform cyber-security standards across government and for stronger reporting and coordination requirements in response to cyber threats.[4] It also underlined the need for a more comprehensive approach to cyber security in the light of Tokyo's anticipated hosting of the 2020 Olympic and Paralympic Games. It was the country's first strategy document to address the potential benefits and dangers posed by the Internet of Things (IoT), a topic on which the government issued a separate document in 2016.[5] It also reiterated the growing role of the MoD in defending against cyber attacks and stressed the importance of closer ties with the United States military under the updated 'Guidelines for U.S.–Japan Defense Cooperation'.[6] The 2015 strategy document was the first to be considered at cabinet level, reflecting a greater recognition of the importance of cyberspace security among the upper echelons of the Japanese government.

The Cybersecurity Strategy released in July 2018 – covering the period 2018–21, with a special emphasis on the Olympic and Paralympic Games – represented a further evolution in Japanese policy.[7] It clearly recognised the potential cyber threat from hostile states, referring on its first page to the growing danger of 'organised, sophisticated, and possibly state-sponsored' cyber attacks. It noted the gradual merging of 'cyberspace and real space' as a result of increasingly sophisticated cyber technologies including artificial intelligence (AI), the IoT, robotics and 3D printers – capabilities at the core of Japan's concept of an information society, or 'Society 5.0' as the government refers to it. The strategy called for improved incident readiness against massive cyber attacks, new initiatives for the protection of critical infrastructure, and enhanced collaboration between stakeholders. Another stated priority was to improve cyber security in the private sector, with a policy of 'Proactive Cyber Defence' including better sharing and utilisation of threat information and system vulnerabilities by businesses.

The 2018 Cybersecurity Strategy also represented a landmark in being the first such document to refer to Japan's deterrence capabilities in cyberspace. It specified that these capabilities should be coordinated by the National Security Secretariat, which provides support to the National Security Council, an inter-agency body established in 2013 to coordinate national-security policies. As yet, however, there is neither an official national military cyber strategy nor an official JSDF military doctrine pertaining to cyberspace in the public domain.

Japan's military cyber journey began in earnest in 2012 with a plan to set up a 100-strong cyber-defence unit,[8] though in previous years the Japanese armed forces had already conducted various cyber-related activities. The most relevant document from which a doctrinal approach can be inferred is the 2019 National Defense Program Guidelines. This emphasised the need for jointness and inter-operability within the JSDF in order to create a multi-domain force that can seamlessly integrate itself into any US defence architecture in East Asia. It also referred to space, cyberspace and the electromagnetic spectrum as domains of warfare. Regarding military operations in cyberspace, its emphasis lay clearly on defence, in line with the JSDF's overall force posture, but it also noted the importance of achieving 'superiority' in the cyber domain and further hinted at the need for offensive cyber capabilities as part of defensive operations to 'disrupt' enemy cyber attacks.[9] Similarly, the 2018 Cybersecurity Strategy stated that acquiring 'capabilities to prevent malicious cyber actors from using cyberspace' should be considered.[10]

Japan's 2020 defence white paper emphasises that cyberspace 'could drastically change the conduct of warfare' and specifically calls for the strengthening of capabilities in order to enable cross-domain operations in space, cyberspace and the electromagnetic domain.[11] While it underlines the need to strengthen cyber-intelligence capabilities, the document also stresses the importance

of 'building the capability to disrupt C4I [command, control, communications, computers and intelligence] of opponents'.[12]

Another crucial document concerning the JSDF's role in cyberspace is the Medium Term Defense Program, which outlined defence priorities for 2019 to 2023.[13] It placed special emphasis on the need to create additional cyber units within the ground forces, which may indicate a particular capability deficit in that branch of the JSDF. The document also underlined the need for better protection of the JSDF's C4I capabilities; for the expansion of the existing cyber-defence unit and the creation of new ones by 2023; and for Japan to participate in bilateral and multilateral cyber exercises.

Governance, command and control

In 2014 the Japanese government began a process of rationalising and improving the civilian command-and-control structure that coordinates cyber activities at the national level. They now resemble those of allied states such as the US and the United Kingdom, although coordination between the public and private sectors remains comparatively weak. Japanese military cyber command and control is less advanced than in allied states.

The groundwork for establishing the current structures was laid in 2014 with the passing of the Basic Act on Cybersecurity (subsequently amended in 2016 and 2018). As a result of this new law, which came into effect in January 2015, the Cyber Security Strategic Headquarters (CSSH) was created, taking over the role of the institutionally weak Information Security Policy Council. Another important body is the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), which acts as the executive organ within the Cabinet Secretariat. Both the CSSH and the NISC have legal authority to coordinate and implement Japan's national cyber-security strategy. The CSSH is officially 'the command and control body of national cybersecurity'.[14] Chaired by the Chief Cabinet Secretary, it also includes the chair of the National Public Safety Commission, the head of the National Police Agency, four ministers (internal affairs and communications; foreign affairs; economy, trade and industry; defense), and eight cyber specialists who chair expert panels.

The CSSH coordinates closely with the Japanese National Security Council and the IT Strategic Headquarters on questions of policy. The NISC in turn coordinates the implementation of policy with the relevant ministries, which share with the providers of critical national infrastructure a legal obligation to report back to the CSSH on cyber-relevant topics.[15] Specifically, the NISC is tasked with integrating and advancing the country's cyber-security strategy, a role which includes developing common standards, protecting infrastructure, developing human resources and implementing a research-and-development strategy.[16]

The second amendment to the Basic Act on Cybersecurity, passed in December 2018 with an eye on security for the Olympic and Paralympic Games, also established a Cybersecurity Council to exchange and collaborate on cyber-security-related information across government, the private sector and academia. Its role is to work in close coordination with the NISC, the national Computer Emergency Response Team (JPCERT) and other institutions such as the National Institute of Information and Communications Technology and the Information-Technology Promotion Agency, both of which aim to promote information-sharing between government and the private sector.[17]

In cyber affairs, Japan's military command-and-control structure remains less advanced than its civilian equivalent. In 2008 the MoD established the C4 Systems Command, reporting directly to the chief of staff of the Joint Staff Office, which was tasked with monitoring the defence of military networks and responding to cyber attacks. The C4 Systems Command reports to the MoD, which in turn cooperates with civilian authorities.

Each branch of the armed forces has a separate cyber-defence unit tasked with network and information-systems defence, principally against internal threats.[18] In March 2019 the JSDF also established the first regional cyber-defence unit as part of the Western Army of the Japan Ground Self-Defense Force (JGSDF), with about 60 personnel. The first of a number of similar regional formations due to be created in the coming years, the unit is tasked with defending and protecting JSDF systems and networks.[19]

A Cyber Defense Group, responsible for coordinating cyber defence across the JSDF as a whole and for

defending its information infrastructure, was created in March 2014. In 2021 it is due to expand from approximately 220 personnel to 290.[20] According to media reports the total number of JSDF personnel deployed in cyber defence will reach 500 by around 2024.[21]

Core cyber-intelligence capability

For a variety of political reasons, including the constitutional arrangements put in place after the Second World War, Japan's intelligence organisations are small and underfunded in comparison to those of other states of similar size. For example, Article 21 of Japan's constitution severely limits the extent to which the government can collect signals intelligence and consequently conduct cyber reconnaissance. Nevertheless, Japan has a suite of relevant organisations, including the Defense Intelligence Headquarters (DIH)[22] and its largest subordinate organisation, the Directorate for Signals Intelligence (DSI). Additionally, Japan has long hosted US signals-intelligence facilities as part of a close intelligence partnership.

The DSI is the equivalent of the National Security Agency (NSA) in the US and Government Communications Headquarters in the UK, though considerably smaller than both. Previously focused on collecting information from communications satellites, the DSI commenced intelligence support to cyber operations in 2012, with assistance from the US through the NSA. At the time, it described these operations as experimental.[23] Budget requests for restructuring and further developing the DSI were submitted for the 2020 fiscal year,[24] but resource choices in favour of expensive weapons platforms, and the Article 21 legal barrier, have so far prevented the establishment of a stronger Japanese signals-intelligence agency.

The total number of JSDF personnel deployed in cyber defence will reach 500 by around 2024

The comparatively well-funded Cabinet Intelligence and Research Office is also likely to play an important role. Reporting directly to the prime minister, it also acts as the coordinating and assessment body for the Japanese intelligence community.

Overall, Japan's indigenous cyber-intelligence capabilities are embryonic, with the country largely reliant on key international partners, especially the US, for its cyber situational awareness and its development of intelligence capabilities.

Cyber empowerment and dependence

Japan remains a world leader in cyberspace technologies. A 2019 study by the International Monetary Fund concluded that the country's digital economy accounted for 49% of its GDP (the figure in the US was 60%, and in China 30%).[25] Of the 51 telecoms or tech companies in the 2020 *Fortune* 'Global 500', the US had 16 and Japan was in second place with ten (just ahead of China with eight, while the combined total for the countries of Western Europe was also eight).[26]

As the pre-eminent producer of industrial robotics[27] and a world leader in the development of digital infrastructure,[28] Japan's economy is both empowered by and increasingly dependent on the ICT sector. The country has an established sovereign microchip-manufacturing capability, with the companies Tokyo Ohka Kogyo Co., Ltd. (TOK), JSR Corporation and Shin-Etsu Chemical together dominating global production of the extreme ultraviolet (EUV) photoresists used in the manufacture of cutting-edge seven-nanometre chips.[29]

Japan is home to the fourth-largest telecommunications group in the world, Nippon Telegraph and Telephone (NTT), which comprises a series of subsidiary branches including NTT Communications (international communications), NTT Domoco (mobile-device communication) and NTT World Engineering Marine Corporation (ground-cable installation and maintenance).[30] According to open-source IPv6 2019 data, the top five internet service providers in Japan are all indigenous: Bbix, Biglobe, Jpne, Mf-native6 and Ocn.[31] NTT World Engineering Marine Corporation's small fleet of cable-laying vessels enables the country to maintain a sovereign and indigenous telecommunications backbone.[32]

Japan is currently lagging behind many other members of the Organisation for Economic Co-operation and Development (OECD) in terms of technological productivity, with an OECD survey suggesting the country needs greater investment in skills and digital

competence – 'particularly for middle-aged and older workers' – in order to close the gap.[33] There is widespread concern about the digital divide between the younger and older generations – a situation illustrated in particularly embarrassing fashion for the government in 2018, when the minister responsible for cyber security was forced to admit he had never used a computer.[34]

Japan has nevertheless formulated a thorough Cyber/Physical Security Framework,[35] and in April 2019 the Ministry of Economy, Trade and Industry launched 'Society 5.0', a national policy aimed at 'integrating cyberspace and physical space in a sophisticated manner'.[36] This initiative set out to implement standards and regulations for governmental and commercial entities operating in cyberspace, and to improve the resilience of the domestic supply chain, as well as to address concerns about Japan's ageing population and shrinking labour force.[37]

In the field of AI, Japan is competitive. It was placed ninth, for example, in a study that ranked the top 50 countries based on their contributions to the two most prestigious AI conferences in 2020.[38] Japanese companies are very active in AI research, with nine of them featuring in a list of the world's leading 100 companies in that regard, compared with six from South Korea and none from India. Nevertheless, the aggregate contribution that Japan's industrial sector makes to AI research still falls behind that of South Korea.[39]

Much of Japan's digital technology has the potential to be further integrated into military applications, although currently that remains little more than a policy aspiration. Japan's annual defence white papers have addressed in general terms the global trend towards digital dependence in military operations, acknowledging the need for the Japanese armed forces to increase the resilience of their command-and-control systems.[40]

In terms of Japan's indigenous satellite capability, the Cabinet Office approved plans to implement and expand the Quasi-Zenith Satellite System (QZSS/*Michibiki*) programme, headed by Japan's Aerospace Exploration Agency, in 2002.[41] The programme launched its first satellite in 2010, followed by three more between 2016 and 2018. Originally designed to augment the functionality of the US Global Positioning System (GPS), the QZSS gives Japan a degree of what the Cabinet Office describes as 'technological sovereignty', as well as bringing a public good to the Asia-Oceania region.[42] The QZSS is currently being reviewed for formal recognition by the Worldwide Radio Navigation System under the auspices of the International Maritime Organization, a process already completed for peers such as GPS, GLONASS (Russia) and *Beidou* (China).[43]

Japan has become very focused on national-security aspects of outer space. It is concerned about North Korea's missile capability and China's growing military power, while remaining keen to expand its own space capabilities. In 2020 it established a Strategic Headquarters for National Space Policy in the Cabinet Office, announced the creation within the Joint Staff of a military unit that would be 'responsible for planning pertaining to joint operations in the space domain',[44] and created a Space Operations Squadron to prepare for the introduction in 2022 of a Space Situational Awareness system.

Cyber security and resilience

Digital and cyber technologies are at the heart of Japan's economy and society, and the overall degree of digital connectedness suggests that a sustained cyber attack on the country's infrastructure would be highly compromising, especially since national cyber resilience is still at a developmental stage.[45]

Japan's efforts to raise its level of resilience in cyberspace were driven principally by security concerns surrounding the planned 2020 Tokyo Olympic and Paralympic Games. The guiding document in that respect was the Cybersecurity Policy for Critical Infrastructure Protection, adopted in April 2018, which focused on the importance of public–private partnerships in boosting resilience and recovering quickly from damage to critical infrastructure caused by cyber attacks.[46] This is unsurprising, as 90% of Japan's ICT assets are in the private sector.[47]

The national-level Computer Emergency Response Team, JPCERT, coordinates with equivalent bodies in other countries and with tactical incident-response teams across the Japanese public and private sectors. The governmental CERT, NISC, also houses the Government Security Operation Coordination Team, which is responsible for accurate and prompt information-sharing across the CERT structure.[48]

In the private sector, the major obstacle to improving cyber resilience is the lack of willingness among companies to share information regarding cyber incidents. This is partly the result of cultural and structural factors. These include a general lack of familiarity with cyber-security issues among senior business leaders, an overreliance on government regulators to establish cyber-security requirements and traditional Japanese business practices that hinder collaboration between companies. According to government statistics, Japanese companies have been slow to integrate cyber security into their corporate governance, especially their risk planning.[49]

The Ministry of Economy, Trade and Industry and one of its subsidiaries, the Information-Technology Promotion Agency, Japan, have published 'Cybersecurity Management Guidelines' for business leaders in an effort to promote cyber-security measures and standards in the private sector.[50] The fact that these guidelines are based on the Cybersecurity Framework of the US National Institute of Standards and Technology illustrates both a tendency towards the adoption of the US view on cyber security and an absence of significant domestic innovation on the issue. Within the Japanese government, a framework for raising cyber-security standards – the Common Standards on Information Security Measures for Government Agencies and Related Agencies – has been in place since 2016.[51] The government's engagement with certain aspects of cyber security since 2006, and the strong ICT sector, probably contributed to Japan being ranked 14th out of 175 countries in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union.[52]

The government has also been holding regular cyber exercises involving both the public and private sectors, some of which have been on quite a large scale – the one in November 2019, for example, had about 5,000 participants.[53] As an example of partnerships with the private sector, in July 2013 the MoD set up a Cyber Defense Council consisting of around ten defence contractors. Its aim is to coordinate exchanges of information between the defence industry and the government, and to organise joint cyber exercises.[54]

Global leadership in cyberspace affairs

Japan has set itself the goal of becoming a leader in cyber diplomacy. Tokyo aims to solidify international rules and norms of behaviour for states in cyberspace and, as part of that norms-based approach, actively promotes the multi-stakeholder model of internet governance. The government has a policy of leading international debate on how to ensure a 'free, fair, and secure cyberspace, strengthening coordination with other countries'.[55] This policy has three pillars: promoting the rule of law in cyberspace, developing confidence-building measures and enhancing international cooperation on capacity-building.

At the global level, Japan has participated in five sessions of the United Nations Group of Governmental Experts[56] and has been promoting the rule of law and confidence-building in cyberspace within the framework of the UN.[57] Tokyo participates in the G7 Cyber Expert Group and various dialogues with regional organisations, such as the ASEAN–Japan Information Security Policy Meeting and the ASEAN–Japan Cybercrime Dialogue.[58] Japan is also a party to the Convention on Cybercrime and actively aims to strengthen international law in that respect by promoting the convention in international forums.[59]

In regional diplomacy, Japan has been partnering with members of the Association of Southeast Asian Nations (ASEAN) on the protection of critical infrastructure and rapid incident response. Tokyo was a leading force in establishing the ASEAN–Japan Cybersecurity Capacity Building Centre, in Bangkok, which facilitates the development of a standardised incident-reporting framework across Southeast Asia,[60] and was also instrumental in setting up the ASEAN Computer Emergency Response Team (ASEAN-CERT).

As one of NATO's global partners and a member of the Partnership for Peace (PfP), Japan became a contributing member of NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE) in March 2019.[61] The CCD COE's mission is to enhance cooperation and information-sharing on cyber defence among NATO members and partners.[62] Japan participated in the CCD COE-led exercise dubbed *Cyber Coalition* 2019 in December 2019; the aim, according to the Japanese MoD, was 'to deepen the knowledge of how to cooperate with NATO on cyber defence' and to improve the 'tactical skills' of the MoD and the JSDF.[63]

Japan's longest and closest international cyber partnership, however, is with the US. The current Japan–US

Cyber Dialogue and the Japan–US Policy Cooperation Dialogue on the Internet Economy are of particular importance to the Japanese government, given that the US is the ultimate guarantor of Japan's security. The Japanese MoD and the Pentagon have established the Cyber Defense Policy Working Group, aiming to deepen information-sharing, organise joint exercises, promote policy discussions and cooperate in training cyber-security experts.[64]

Japan has CERT cooperation agreements with other Asian countries, including India, and with Australia. Japanese CERT officials meet annually with Chinese and South Korean counterparts, and also cooperate with the Asia-Pacific Computer Emergency Response Team (APCERT) on the TSUBAME project, a traffic-monitoring system that shares data between 23 national CERTs.[65] Japanese CERTs cooperate effectively with their US counterparts, and with others in the Asia-Pacific region, but less so with those in Europe.

Japan has established bilateral cyber dialogues with 11 countries – Australia, Estonia, France, Germany, India, Israel, Russia, South Korea, Ukraine, the UK and the US – and also with the European Union (EU) and NATO. Besides participating in the ASEAN–Japan Cybersecurity Policy Meeting, where the focus is on capacity-building, Japan also holds trilateral cyber discussions with China and South Korea, focusing on North Korean operations.[66] The UK and the EU have dialogues with Japan at the ministerial and expert levels, as well as technical cooperation and joint capacity-building.[67] Japan and the EU have also been jointly promoting better data protection, with the European Commission having agreed with Japan on arrangements for data exchange without further reference to national authorities for approval – a move that facilitates the gradual streamlining of data-privacy standards.[68]

Japan's longest and closest international cyber partnership is with the US

Offensive cyber capability

The development of any offensive military capability is constrained by Japan's military history and by current views on the post-Second World War pacifist constitution. Article 9 of the constitution denies the country the right to military forces of any kind. Though this has been ignored since 1954, when the Self-Defense Forces Act was passed, every government has had to make complex legal and political arguments to massage public opinion each time the reach and mission of Japan's forces have been extended. Since 2015 the government has made additional reinterpretations to make it possible, under certain circumstances, to come to the aid of an ally even if Japan itself is not under attack.[69] This shift is now also seen as allowing collective self-defence and active defence in cyberspace.[70]

At the same time, there have been hints in official documents of a subtle shift in Japanese policy from focusing purely on defence to developing offensive capabilities, for which there has been a low-key push by the JSDF.[71] The 2020 defence white paper states that the armed forces would act to disrupt enemy cyber operations during an attack on Japan.[72] Some senior policymakers have also suggested that offensive cyber is being considered as a way of providing a 'deterrence by punishment' option for Japan, including as part of its missile-defence strategy. However, this would require Japan's Self-Defense Forces Law to be revised.[73]

The fact remains that, for the foreseeable future, Japan will probably remain reliant on its alliance with the US for any kind of offensive response to a cyber threat. It is notable that the 2015 guidelines for US–Japan defence cooperation[74] include an entire section dedicated to cyberspace, setting out the circumstances under which the US can lend cyber support in Japan's defence. The narrowest interpretation of the text would limit US assistance to the protection of Japanese critical information infrastructure used by US forces in Japan, but in the broadest interpretation the text is analogous to NATO's Article 5, with a serious cyber attack on Japan being treated like an attack on the US.

Notes

1 Information Security Council, *The First National Strategy on Information Security: Toward the Realisation of a Trustworthy Society*, 2 February 2006, http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

2 Information Security Council, *Cybersecurity Strategy: Towards a World-Leading, Resilient and Vigorous Cyberspace*, 10 June 2013, http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf.

3 Japan Ministry of Foreign Affairs, *National Security Strategy*, 17 December 2013, http://japan.kantei.go.jp/96_abe/documents/2013/__icsFiles/afieldfile/2013/12/17/NSS.pdf.

4 Government of Japan, *Cybersecurity Strategy*, 4 September 2015, http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

5 National Center of Incident Readiness and Strategy for Cybersecurity, *General Framework for Secure IoT Systems*, 26 August 2016, http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf.

6 US Department of Defense, 'The Guidelines for U.S.–Japan Defense Cooperation', 27 April 2015, https://archive.defense.gov/pubs/20150427_--_GUIDELINES_FOR_US-JAPAN_DEFENSE_COOPERATION.pdf. The 'guidelines' framework has been used since 1979 to set the parameters of defence cooperation between the two countries.

7 National Center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity Strategy*, 27 July 2018, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

8 Richard J. Samuels, *Special Duty: A History of the Japanese Intelligence Community* (Ithaca, NY: Cornell University Press, 2019), pp. 228–9.

9 Ministry of Defense, *National Defense Program Guidelines for FY 2019 and beyond*, 18 December 2018, https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf.

10 National Center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity Strategy*, 27 July 2018.

11 Ministry of Defense, *Defense of Japan 2020*, 2020, p. 41, https://www.mod.go.jp/e/publ/w_paper/wp2020/DOJ2020_EN_Full.pdf.

12 *Ibid*., pp. 218, 267.

13 Ministry of Defense, *Medium Term Defense Program (FY 2019 – FY 2023)*, 18 December 2018, https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/chuki_seibi31-35_e.pdf.

14 Government of Japan, *Cybersecurity Strategy*, 4 September 2015.

15 These include: 'the network-based vigilance and monitoring of malicious activities against information systems of administrative organs; fact-finding on the cause of incidents and audit of relevant governmental bodies; information gathering and analysis on domestic and foreign cybersecurity; the promotion of international cooperation and collaboration; and cybersecurity workforce development for and by the governmental bodies'. National Center of Incident Readiness and Strategy for Cybersecurity, *Organisational Structure*, http://www.nisc.go.jp/about/organize.html.

16 National Center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity Framework in the Government of Japan* (handout), September 2019.

17 *Cyber Security Strategy in Japan: Present Situation and Challenges*, presentation delivered by Tomoo Yamauchi, Deputy Director-General, NISC, to the Foreign Press Center of Japan, 4 July 2019, https://fpcj.jp/wp/wp-content/uploads/2019/07/190704-Cybersecurity-StrategyForeign-Press-Center-1.pdf.

18 Ministry of Defense, 'Regarding Response to Cyber Attack', undated, https://www.mod.go.jp/e/publ/answers/cyber/index.html.

19 Franz-Stefan Gady and Yuka Koshino, 'Japan and Cyber Capabilities: How Much Is Enough?', Military Balance blog, International Institute for Strategic Studies, 28 August 2020, https://www.iiss.org/blogs/military-balance/2020/08/japan-cyber-capabilities.

20 'Japan Embraces AI Tools to Fight Cyberattacks with US$237 Million Investment', *CISO Magazine*, 6 April 2020, https://cisomag.eccouncil.org/japan-embraces-ai-tools-to-fight-cyberattacks-with-us237-mn-investment.

21 Daishi Abe, 'Lagging China and the US, Japan to beef up cyberdefense', Nikkei Asia, 20 June 2020, https://asia.nikkei.com/Politics/Lagging-China-and-the-US-Japan-to-beef-up-cyberdefense.

22 DIH is Japan's largest intelligence organisation, with around 2,000 personnel in 2020.

23 Samuels, *Special Duty: A History of the Japanese Intelligence Community*, p. 232.

24 Ministry of Defense, *Defense Programs and Budget of Japan: Overview of FY2020 Budget Request*, 2019, https://www.mod.go.jp/e/d_act/d_budget/pdf/200225a.pdf.

25 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.

26 For technology companies in 2020, see https://fortune.com/global500/2020/search/?sector=Technology. For telecoms

companies in 2020, see https://fortune.com/global500/2020/search/?sector=Telecommunications.

27 Hiroshi Fujiwara, 'Why Japan leads industrial robot production', International Federation of Robotics (IFR), 17 December 2018, https://ifr.org/post/why-japan-leads-industrial-robot-production.

28 OECD, *Japan*, OECD Economic Surveys, April 2019, p. 44, https://www.oecd-ilibrary.org/economics/oecd-economic-surveys-japan-2019_fd63f374-en.

29 Osamu Tsukimori, 'Japanese manufacturers use decades of experience to dominate key chemical market for cutting edge chips', *Japan Times*, 9 October 2019, https://www.japantimes.co.jp/news/2019/10/09/business/japanese-manufacturers-use-decades-experience-dominate-key-chemical-market-cutting-edge-chips/#.Xc7ePS10eHo.

30 Nippon Telegraph Telephone (NTT) Group, https://www.ntt.co.jp/index_e.html.

31 Ipv6 Test, 'IPv6 in Japan', October 2019, https://ipv6-test.com/stats/country/JP.

32 NTT WE Marine, 'Cable-Laying Vessels', https://www.nttwem.co.jp/english/ship.

33 OECD, *Japan*, OECD Economic Surveys, April 2019, p. 44.

34 BBC News, 'Japan's cyber-security minister has "never used a computer"', 15 November 2018, https://www.bbc.co.uk/news/technology-46222026.

35 Ministry of Economy, Trade and Industry, *The Cyber/Physical Security Framework: To ensure trusthworthiness of a new type of supply chain in 'Society 5.0', so-called 'value creation process'*, 18 April 2019, https://www.meti.go.jp/english/press/2019/pdf/0418_001b.pdf.

36 Ministry of Economy, Trade and Industry, *Cyber/Physical Security Framework (CPSF) Formulated*, 18 April 2019, https://www.meti.go.jp/english/press/2019/0418_001.html.

37 *Ibid.*

38 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.

39 *Ibid.*

40 Ministry of Defense, *Defense of Japan 2019*, 2019, p. 229, https://www.mod.go.jp/e/publ/w_paper/wp2019/pdf.

41 Cabinet Office, 'Juntenchōeisei shisutemu ni tsuite', undated, https://www8.cao.go.jp/space/qzs/qzs.html.

42 Quasi-Zenith Satellite System (QZSS), 'Overview of the Quasi-Zenith Satellite System (QZSS)', https://qzss.go.jp/en/overview/services/sv01_what.html.

43 Quasi-Zenith Satellite System (QZSS), '[Report] Deliberations on QZSS at the 7th Session of the IMO's NCSR', 5 March 2020, https://qzss.go.jp/en/events/imo_200305.html.

44 Ministry of Defense, *Defense of Japan 2020*, pp. 266–7.

45 National Center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity Strategy*, 27 July 2018.

46 National Center of Incident Readiness and Strategy for Cybersecurity, 'Summary of Cybersecurity Policy for CIP (4th Edition)', 25 July 2018, https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_summary.pdf.

47 Mihoko Matsubara, 'A Glimpse into Private Sector Security in Japan', Lawfare, 26 June 2018, https://www.lawfareblog.com/glimpse-private-sector-cybersecurity-japan.

48 National Center of Incident Readiness and Strategy for Cybersecurity, 'The Guidance on Operations of Information Security Measures of Government Agencies and Related Agencies', 31 August 2016, Revised 25 July 2018, https://www.nisc.go.jp/eng/pdf/shishin30-en.pdf.

49 Information Technology Promotion Agency, 'Fact-finding survey on corporate CISOs and promotion of security measures', 25 March 2020, https://www.ipa.go.jp/security/fy2019/reports/2019DL_index.html.

50 Ministry of Economy, Trade and Industry, 'Cybersecurity Management Guidelines Revised', press release, 16 November 2017, https://www.meti.go.jp/english/press/2017/1116_001.html.

51 National Center of Incident Readiness and Strategy for Cybersecurity, 'The Guidance on Operations of Information Security Measures of Government Agencies and Related Agencies'.

52 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

53 'Jūyō infura 14 bun'ya ni yoru bun'ya ōdan-teki enshū o kaisai, yaku 5, 000-mei ga sanka (NISC)', ScanNetSecurity, 12 November 2019, https://scan.netsecurity.ne.jp/article/2019/11/12/43217.html.

54 'Inauguration and Initiatives of the Cyber Defense Council', *Japan Defense Focus*, no. 44, September 2013, https://www.mod.go.jp/e/jdf/sp/no44/sp_activities.html#article03.

55 Ministry of Foreign Affairs, Cybersecurity presentation, undated, https://www.mofa.go.jp/files/000412327.pdf.

56 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.

57 United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

58 Ministry of Defense, *Defense of Japan 2019*.

59 Council of Europe, 'Japan joins Budapest Convention', press release, 3 July 2012, https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/japan-joins-budapest-convention?inheritRedirect=false.

60 'Asean cybersecurity centre opens in Bangkok', *Bangkok Post*, 14 September 2018, https://www.bangkokpost.com/world/1540082/southeast-asian-cyber-security-centre-opens-in-thailand.

61 NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), 'Japan to Join the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn', press release, 12 January 2018, https://ccdcoe.org/news/2018/japan-to-join-the-nato-cooperative-cyber-defence-centre-of-excellence-in-tallinn.

62 NATO Cooperative Cyber Defence Centre of Excellence, 'About Us', https://ccdcoe.org/about-us.

63 Ministry of Defense, 'Participation in NATO Cyber Defence Exercise "Cyber Coordination 2019"', press release, 27 November 2019, https://www.mod.go.jp/j/press/news/2019/11/27a.html.

64 Ministry of Defense, *Defense of Japan 2019*.

65 Asia Pacific Computer Emergency Response Team, 'TSUBAME Working Group', https://www.apcert.org/about/structure/tsubame-wg/index.html.

66 The latest trilateral dialogue was held in December 2020. See Ministry of Foreign Affairs of Japan, 'The 5th Trilateral Cyber Policy Consultation', 10 December 2020, https://www.mofa.go.jp/press/release/press24e_000019.html.

67 Wilhelm M. Vosse, 'Japan's Cyber Diplomacy', Research in Focus, EU Cyber Direct, October 2019, https://eucyberdirect.eu/wp-content/uploads/2019/10/vosse_rif_topublish.pdf.

68 European Commission, 'European Commission adopts adequacy decision on Japan, creating the largest area of safe data flows', press release, 22 January 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421.

69 Franz-Stefan Gady, 'Toothless tiger: Japan Self-Defence Forces', BBC News, 14 October 2015, https://www.bbc.com/news/world-asia-34485966.

70 See Daisuke Akimoto, 'Cybersecurity and Japan's Right to Self-Defense', Institute for Security and Development Policy, undated, https://isdp.eu/cybersecurity-japans-right-to-self-defense.

71 Also, in 2019, according to a media report, the Ministry of Defense contracted private-sector companies to develop offensive cyber capabilities for defensive purposes. See 'Japan to develop 1st defense use computer virus against cyberattacks', *Kyodo News*, 30 April 2019, https://english.kyodonews.net/news/2019/04/e9e4df950d3d-japan-to-develop-1st-defense-use-computer-virus-against-cyberattacks.html.

72 Ministry of Defense, *Defense of Japan 2020*, p. 218.

73 See Franz-Stefan Gady and Yuka Koshino, 'Japan and Cyber Capabilities: How Much Is Enough?', Military Balance blog, International Institute for Strategic Studies, 28 August 2020, https://www.iiss.org/blogs/military-balance/2020/08/japan-cyber-capabilities.

74 US Department of Defense, 'The Guidelines for U.S.–Japan Defense Cooperation'.

8. China

China's leaders have moved decisively to embrace the information revolution. They started from a position of relative backwardness in electronics in the 1990s, but with the advantages of a rapidly growing economy and technology transfer from abroad. The country has since established the world's most extensive cyber-enabled domestic surveillance and censorship system, which is tightly controlled by the leadership. China's intention of becoming a cyber power was reflected in its military strategy released in 2015 and its first formal cyber-security strategy in 2016. The country has ambitious goals for the indigenous manufacture of the core internet technologies it relies on, aiming to become a world leader in such technologies by 2030. Its core cyber defences remain weak compared with those of the United States, and cyber-resilience policies for its critical national infrastructure are only in the early stages of development. China has been locked in a battle with the United States and its allies over global cyber governance since the early 2000s, a contest aggravated by US determination to sanction Chinese tech firms in response to China's malicious behaviour in cyberspace. Since the early 2000s China has conducted large-scale cyber operations abroad, aiming to acquire intellectual property, achieve political influence, carry out state-on-state espionage and position capabilities for disruptive effect in case of future conflict. China is a second-tier cyber power but, given its growing industrial base in digital technology, it is the state best placed to join the US in the first tier.

Strategy and doctrine

China's strategic approach to the security aspects of cyberspace has been dominated by its perception of the ideological, economic and military threat from the United States: the early development of US military cyber doctrine in the 1990s; the use of cyber in US military campaigns in Kosovo in 1999 and Iraq in 2003; and US support for the internet-based political revolts in states in the former Soviet bloc and North Africa.

From the outset, China's main strategic preoccupation in cyberspace has been domestic – to prevent the spread of Western liberal thinking via the internet. From 2003 onwards, at the United Nations, it advocated the principle of 'cyber sovereignty' whereby states would be able to exert more control over their 'sovereign' portion of the internet. It was also in 2003 that China began implementing its 'Golden Shield Project', a programme of internet-based internal surveillance and censorship that became known as the Great Firewall of China – an attempt to exert sovereign control. As part of this, from 2009 onwards China undertook efforts to block certain US software applications (such as Facebook, Twitter and YouTube) because of conflicts with its censorship laws.

List of acronyms

BRI	Belt and Road Initiative
CAC	Cyberspace Administration of China
CCP	Chinese Communist Party
ICT	information and communications technology
MPS	Ministry of Public Security
MSS	Ministry of State Security
PLA	People's Liberation Army
SSF	Strategic Support Force

In 2013, after ten years of partial reforms aimed at enhancing the country's cyber capabilities, the leaders of the Chinese Communist Party (CCP) were shocked by the revelations in the leaks by US defector Edward Snowden. The leaks made clear the continuing gulf between the US and China on cyber capability, and particularly the weakness of China's cyber defences (in terms of protecting networks rather than controlling content). In 2014 President Xi Jinping instigated a wave of internet-related organisational reforms and new laws and regulations, with the aim of making China a cyber power. This included reconfiguring and assuming personal leadership of the main CCP body in charge of cyber policy[1] and establishing a new government body alongside it, the Cyberspace Administration of China (CAC). Numerous cyber-related strategies and measures for the civil sector followed. China's first national Cyberspace Security Strategy was published in 2016[2] and was supported by China's first Cybersecurity Law in 2017.[3] The strategy set nine core tasks, with a heavy emphasis on sovereignty and improving cyber-defence enablers (industry and education).[4]

On the industry side, the 'Made in China 2025' strategy, announced in 2015, is of particular significance. Identifying reliance on foreign vendors for its core internet technology as China's biggest cyber risk, this ambitious strategy intended to ensure that 70% of the core internet technology the country depended on would be manufactured domestically by 2025, and that it would become a world leader in such technology by 2030. This is complemented by the Belt and Road Initiative (BRI), in which the Digital Silk Road component is designed to open up markets in the developing world to Chinese technology.

By 2020, many of these policy measures had begun to bear fruit, including a reported decline in the incidence of domestic cyber crime.[5] But serious issues remained, including a reported doubling of intrusions into Chinese websites, with government sites a particular target.[6] Implementation of the cyber strategy has been hampered by various constraints, the biggest internal one being the low priority given to cyber-security skills in China's education system and training institutions.[7] The main external impediment has been the intensifying campaign by the US and its allies to constrain China's cyber-industrial ambitions, with the ban on sales of microchip technology to Huawei a prime example of US and allied tactics. It is not yet clear how damaging these tactics will be. They may push China to redouble its Made in China 2025 effort, to exploit the potential of its massive internal market (the country has one billion of the world's estimated four and a half billion internet users), and to step up sales of Chinese technology to the developing world through the BRI.

The other key dimension to China's cyber strategy since the early 2000s has been its use of cyber operations abroad for strategic effect. These have included industrial-scale espionage operations designed to acquire both commercial intellectual property and personal data. China has also actively used disruptive cyber operations, while being careful to pitch them below the threshold that might trigger an escalatory response – its attempts to influence electoral processes in Taiwan are one example.

China's strategy and doctrine for the military use of cyber capabilities date from the early 2000s, with its 2004 focus on 'Winning Local Wars under Informatised Conditions' an early example.[8] This strategy envisioned the incorporation of information technology into every facet of military activity, with the information domain seen not as separate but as integral to the land, air and sea domains. By 2005 this had redefined Chinese military doctrine, which stated that the protection or destruction of information systems would be a 'method of war' for the People's Liberation Army (PLA).[9]

It is important to note that Chinese military doctrine views 'network'-related activities (what most other states call 'cyber operations') as a component of information war.[10] The Chinese military sees information warfare as a struggle against adversaries to dominate the production and flow of information in order to support its strategic goals. Achieving this in a conflict environment – while degrading or constraining adversaries' efforts – is termed 'information dominance'.[11]

This is closely linked to the Chinese concept of 'systems confrontation', informed by the Chinese perception that the US defeated Iraq in the First Gulf War (1990–91) by destroying Iraq's operational command-and-control system.[12] As set out in China's *The Science of Military Strategy*, pre-emption is also a long-standing and

fundamental part of Chinese military thinking and has become even more prominent in 'information war': vulnerability to a paralysing attack on one's own command-and-control system places a premium on a first strike.[13]

This thinking has matured under Xi's leadership. One example is China's first military strategy to recognise the centrality of cyberspace in strategic and military policy, published in 2015, which stated that information would play a leading role in any conflict rather than being merely an enabler.[14] By 2019 numerous PLA sources were referring to the possibility that the acceleration of changes in military strategy, combined with new technological opportunities, would lead to an arms race in 'intelligentisation', meaning the use of artificial intelligence (AI) in military operations, intelligence collection and decision-making.[15]

The SSF will improve China's war readiness

The transitions foreshadowed in such doctrinal statements will take a long time to implement. As part of its aspiration to have a 'world class military' by 2050, China has set out a timetable to 2035 for the organisational reforms, including changes to force structure, that might turn doctrine into reality in the cyber realm.[16] Like the US, China is pursuing a strategy of information dominance in cyberspace, but acknowledges that its armed forces will need to undergo a transformation before that goal is reached.[17]

Governance, command and control

Since 2014, Xi has been at the top of the chain of command for all matters concerning cyberspace, both civilian and military. His organisational changes to cyber policy in the civil and military sectors suggest that he wanted to accelerate the transformations and score some early successes in reducing the vulnerability of Chinese networks to infiltration and attack.

On the civilian side, the CAC has become the focal point of all cyberspace policy, although powerful independent nodes remain – such as the Ministry of Public Security (MPS), the Ministry of State Security (MSS) and the Ministry of Industry and Information Technology. The CAC has formalised the new agenda through national legislation and by setting up offices in each of the country's 31 provincial-level administrations.

In the military cyber sphere, in 2015 Xi established the Strategic Support Force (SSF), where most of the PLA's cyber capabilities are now centred. This was part of system-wide reforms to the PLA's force structure, administration and command-and-control mechanisms. The SSF was not a new force created from scratch but instead the result of the restructuring of existing units from across the armed forces, consolidated under a single command structure.[18] Today the SSF consists of two main elements: the Space Systems Department, responsible for space operations, and the Network Systems Department, responsible for strategic information operations.

The creation of the SSF is significant: not only does it report directly to China's paramount military decision-making body, the Central Military Commission, but it has also combined disparate capabilities into an integrated whole. Previously the PLA's information-operations units had been grouped according to mission type – namely reconnaissance, attack, defence and psychological warfare. For example, cyber espionage and signals intelligence had been handled by the now-defunct Third Department of the General Staff; offensive cyber operations and electronic countermeasures had been siloed in the former Fourth Department; psychological warfare had been the responsibility of the General Political Department; and most aspects of military network security had been managed by the General Staff Department's Informatisation Department.

Consolidating these functions into the SSF reflects the PLA's new conception of space, cyber and the electromagnetic spectrum as a unique warfighting domain rather than adjunct functions serving other forms of combat.[19] The implications of the SSF for China's military cyber capability are twofold. Firstly, a more unified force will be able to prosecute the type of complex, multidimensional information operations that the PLA foresees in future conflicts. Psychological, electronic, cyber and kinetic actions can be incorporated into a single information-warfare strategy, each deployed for specific effects at different points in a crisis or conflict.[20]

Secondly, in terms of warfighting, the SSF will improve China's war readiness and help the PLA shift more smoothly from a peacetime to a wartime

posture. By combining espionage and attack functions across electronic-, cyber- and space-warfare units, and by bringing them under a single command, the PLA aims to survey the battlefield, prepare combined-arms operations and develop specific capabilities that can be continuously adapted to match the requirements of fast-moving situations.[21] This includes malware and other cyber weapons, which can be developed, refined and deployed in a continuous loop that draws on both reconnaissance and offensive functions.

While the SSF has subsumed the PLA's strategic information-warfare units, there are still units with related functions that are attached to the single services and continue to operate within the PLA's newly created joint-theatre commands. It is unclear how effectively these units could operate alongside the SSF, and whether they have a national mission or are able to coordinate and de-conflict their respective missions during operations. According to a PLA assessment of SSF reforms, 'cross-unit forces transfer and handover are progressing smoothly; new adjustment and formation of units are being completed and delimited according to plan; the system of systems architecture and contours of new-type combat forces is starting to appear'.[22] While this authoritative assessment suggests optimism on the part of the PLA, it also indicates that reforms are at an early stage, which is likely to limit the SSF's ability to conduct multidimensional information-warfare operations in the short to medium term.

Core cyber-intelligence capability

China has unsurprisingly organised its intelligence agencies according to its unique political system and strategic needs. The priorities of the intelligence agencies include sustaining the rule of the CCP, public order, economic and commercial intelligence, scientific and technical intelligence, military intelligence and covert operations (with the latter including political-influence operations).

These intelligence goals are pursued by competing bureaucracies. Some are stand-alone, dedicated intelligence and security agencies such as the MSS,[23] the MPS and, within the PLA, the SSF. But unlike their counterparts in Western countries, these agencies all have significant operational roles in delivering internal security. They are complemented by the intelligence-analysis work carried out by key departments of the CCP such as the Office for Taiwan Affairs, the United Front Department, the Central Cyberspace Affairs Commission,[24] the Central Commission for Politics and Law and the Central Military Commission.

Partly in reaction to the process of opening up to the world through internet access and the increase in international exchanges of all kinds, and partly because of enduring regime preferences, China has built the world's most powerful domestic surveillance system. Its domestic intelligence capability depends not just on the agencies described above but also on a complex web of enforcement mechanisms that operate in parallel. One of the most important is the Central Discipline and Inspection Commission of the CCP, which collects intelligence on leading members of the party. Another is the web of CCP committees that extends throughout all levels of government, large commercial enterprises, hospitals, schools and universities. In addition, the Golden Shield Project, launched in 2003, involves the use of information and communications technology (ICT) to transform the way China's security services collect, analyse and transmit information. China has also implemented a range of other initiatives to enhance its surveillance capabilities, including Skynet, a massive video-surveillance network that comprises at least 200 million cameras nationwide,[25] and Sharp Eyes, an extension of the Skynet network that focuses on rural areas and leverages big data and AI for social control.[26]

China also has a nationwide system that aspires to consolidate data from street-level surveillance platforms, private and public services, and the digitised records that the party-state maintains on every citizen, aiming to allow the authorities to track individuals in real time as they move across offline and online spaces. From the publicly available evidence, it is not clear how comprehensive this system is or how effective it has been.

While China's core cyber-intelligence capabilities are therefore formidable domestically, it has also developed and extensively used cyber for overseas espionage. These intelligence efforts are often characterised in terms of their volume rather than sophistication, with Chinese intrusions featuring heavily among those detected and attributed by Western intelligence agencies and cyber-security companies. That said, China

may have learned from the sophisticated Western intelligence capabilities revealed in the Snowden leaks, and may now possess more advanced capabilities either held in reserve or hidden in the sheer volume of its other operations.[27]

China's analysis and dissemination of intelligence is less mature than that of the US and its key allies. While some security officials have suggested that there is now an unmanageable glut of data generated by 'informatised' surveillance, the information ecosystem in China remains highly politicised and therefore difficult to reform. It is characterised not just by a repressive and closed institutional disposition and organisational culture, but also by the ferocity and intensity of the anti-corruption campaign that Xi has led since he took office as head of the CCP in November 2012. This campaign has purged thousands of officials from the intelligence and security agencies, including many at senior levels. Chinese intelligence analysis is very different from the systems operating in the US, the United Kingdom and in many other Western governments: it remains ideology-driven and is increasingly enmeshed with questions of prestige around the political goals of the CCP leaders, making it less independent from political influence than its Western equivalents.

Cyber empowerment and dependence

China's participation in the globalised ICT industrial sector began in 1984 and was boosted by relationships with corporations based in the US (initially Motorola, and later Microsoft). The sector expanded dramatically once China had secured US agreement for public connectivity to the internet and the World Wide Web in 1995. A major force behind this expansion was former Chinese leader Jiang Zemin, who consistently advocated industrial transformation through electronics and information technology. By 2000, due in part to Jiang's leadership, China regarded the information society as an all-encompassing phenomenon that would be crucial for its future prosperity and security.[28] By then, the still-nascent private sector was also playing a role in the digital-technology sector, with Alibaba starting up in 1999 and the emerging computer company Lenovo getting a huge boost in 2005 when it acquired the desktop business of global tech giant IBM. Jiang's successors have subsequently increased the momentum, and under Xi there have been two particularly important developments: his 2014 declaration of China's aim of becoming a cyber power and the government launch, in 2015, of the Made in China 2025 industrial strategy.

A government white paper in 2020 stated that China had moved from a period of rapid development of its indigenous ICT industry to one in which there would be a deep and integrated digitisation of the economy and society.[29] It was not alone in this assessment. The International Monetary Fund has highlighted China's world-leading position in e-commerce and in some aspects of FinTech, describing its rate of digitisation as the fastest in the world.[30] The scale of China's value-added digital economy reached RMB 35.8 trillion (US$5.12trn) in 2019, accounting for 36.2% of GDP – a higher share than in countries such as Brazil, India and South Africa but still far behind the US (50%).[31] China's fast-expanding ICT sector was valued in 2019 at RMB 7.1trn (US$1.02trn), or just over 7% of GDP. Provinces with the most developed digital economies enjoyed the highest rates of economic growth (Beijing, Fujian, Guangdong, Shanghai and Zhejiang, for example).

China's influence in the global ICT economy has risen commensurately, including through its development of online platforms. The China Academy of Information and Communications Technology said in 2020 that with the online-platform sector, led by Alibaba and Tencent, the country's role had changed from 'imitation and catch-up' to 'leading global innovation'.[32] Before the US moved against it in 2020, the Chinese-owned company TikTok had set off a global short-video boom.

Overall, however, a large obstacle in the way of China's cyber empowerment is its ongoing dependence on foreign vendors for core internet technology, despite the Made in China 2025 strategy and indeed the emphasis science-and-technology policy has placed on self-reliance ever since the founding of the People's Republic. The Chinese media has coined the phrase 'eight guardian warriors' to refer to the US companies that remain enmeshed in China's telecommunications infrastructure: Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle and Qualcomm.[33] The issue was underlined in 2020 by the US using its domination of the global microchip industry to undermine Huawei.

Indeed, in a sign that China views its reliance on foreign technology companies as likely to be long term, some of them – including Cisco, IBM, Intel and Microsoft – were invited to join China's leading consultative group for writing national standards related to cyber security. The move gives China better oversight of the use of US technology in its networks. Meanwhile, despite multiple attempts to move away from Microsoft Windows, China is yet to develop its own operating system to replace those of Microsoft or Apple.[34]

One of the technologies prioritised by Xi as part of the Made in China 2025 strategy is AI. In 2017 the government issued its first development strategy specifically for AI, aiming for China to become a world leader in the field by 2030.[35] A summary of the 14th five-year plan (2020–25), released in October 2020, emphasises investment in home-grown innovations and includes AI in a list of 'forward-looking and strategic' technologies alongside quantum communications, integrated circuits and biological engineering.[36] Chinese firms are leaders in some aspects of AI, especially concerning facial recognition, but otherwise lag far behind Microsoft and Google. The US still leads in developing the foundational platform and support architecture of AI, for example developing 66% of global AI open-source software compared with China's 13%.[37] The level of private-equity investment in AI in China is still far below that in the US, which has accounted for two-thirds of the global total since 2011.[38] China was placed second, behind the US, in a ranking of the top 50 countries according to their contributions to the two most prestigious AI conferences in 2020.[39] The story is similar for quantum computing: in 2017 Chinese scientists succeeded in entangling ten superconducting qubits, breaking Google's prior world record of nine, but since then Google has claimed a 54-qubit machine (in 2019) and IBM has developed something similar. Nevertheless, China may be a world leader in research and development (R&D) associated with quantum communications, having declared the installation of the world's longest quantum-communications cable (2,000 kilometres) between Beijing and Shanghai, as well as a connection via satellite over a smaller distance.[40] Chinese researchers announced in 2021 that a 4,600-km quantum-communications network was ready for use after two years of experimental operations.[41]

Space-based platforms related to cyber are an area where China has achieved greater self-reliance. Its total satellite fleet numbers 410.[42] It operates a large-scale space-based intelligence, surveillance and reconnaissance (ISR) capability, drawing on a fleet of 132 dedicated military satellites that is the second largest in the world after that of the US.[43] According to a 2019 report from the US Defense Intelligence Agency, China's ISR satellites are capable of offering electro-optical and synthetic aperture radar (SAR) imagery as well as electronic and signals-intelligence data.[44] They include the dual-use *Yaogan* satellite fleet[45] and the *Haiyang* series of ocean satellites, which provide global identification and tracking for military and civilian vessels.[46]

China has also developed a sovereign capability in satellite navigation through its *Beidou* system, rivalling the United States' GPS and, importantly, ending Chinese dependence on the US system for guiding its own missiles. The *Beidou* network had covered the entire Asia-Pacific region by 2012 and achieved global coverage by mid-2020. Chinese military analysts acknowledge that as China follows the US into reliance on space- and cyber-based capabilities, it will inevitably come to have the same vulnerabilities during conflict.[47]

Chinese firms are leaders in some aspects of AI, but otherwise lag far behind Microsoft and Google

In summary, China has made significant progress in developing an indigenous digital-industrial base but – given US dominance of global microchip supply,[48] as illustrated during the US–China trade war launched by the Trump administration – it is likely to remain fundamentally reliant on the US for its core internet technology for the foreseeable future. China has some advantages, for example an enormous internal market that provides solid foundations for winning a substantial portion of the developing world's digital market. But it is notable that in 2019, in contrast to some of his previous rhetoric, Xi described the task facing China as a new 'Long March',[49] seemingly an acceptance of the time and effort it will take to overcome the challenge posed by the US.

Cyber security and resilience

Information security has been a priority for the Chinese government since the 1990s, yet for much of that time the focus has been on 'content security', namely the censoring of politically subversive information in cyberspace. Beijing's preoccupation with content – rather than the physical networks that transport it – reflects the party-state's conception of state security, which is more expansive and ideological than Western notions of national security. China's leaders see the security of the regime as constantly under threat.[50] It is likely that the focus on promoting content security to meet censorship objectives has diminished efforts to advance other forms of network-centred (cyber) security, and that this constraining effect will persist.

A succession of shocks has produced a sea change in China's approach to network security. In 2013, apart from the Snowden leaks, China had to deal with the humiliating exposure of a PLA cyber-espionage unit (61398) by Mandiant, a US cyber-security firm, which revealed deeply concerning gaps in the Chinese military's cyber security. Meanwhile, the eavesdropping on China's top leaders ordered by the disgraced former internal-security chief Zhou Yongkang in 2012 had highlighted the vulnerability of leadership communications and the dangers of a cyber-espionage capability beyond central control.[51]

Beijing's own assessments of its cyber security have been sober

Beijing's own assessments of its cyber security have been sober. A 2017 report by the National Computer Network Emergency Response Technical Team (CNCERT) stated that attacks from foreign states (advanced persistent threats) were frequent and becoming 'normal', and were directly threatening national security.[52] The report referred to serious damage to data and rampant fraud, noting that the number of attacks against industrial control systems was increasing, with many important safety incidents.[53] In September 2020, the six-monthly report released by the China Internet Network Information Center noted that personal cyber security had improved, especially in the area of online fraud, but the country's overall cyber-security situation had worsened.[54] It reported a significant increase in the number of websites affected, some of which were infected with 'backdoors'.[55] Also, the number of vulnerabilities identified in high-risk systems more than doubled from the previous year.[56]

The sheer number of new institutions, laws, regulations and announcements since 2014 suggests that China is still in the early stages of building its cyber resilience and contingency measures. Government, industry and academia have begun institutionalised exchanges through the Cybersecurity Association of China, created in 2016, which reportedly aligns the three sectors around a common set of objectives.[57] Also in 2016, Beijing announced a major reform of its national cyber-standards committee, the National Information Security Standardisation Technical Committee (NISSTC), with representatives from across government, from hundreds of Chinese companies and from a much smaller number of foreign companies. By 2018 the NISSTC had published more than 300 new cyber-security standards, covering critical-information-infrastructure protection, product review and other areas.[58] In December 2019, the Multi-level Protection Scheme 2.0 (MLPS 2.0) was implemented, broadening the scope for regulation of network operators and imposing heightened regulatory requirements.[59] To strengthen the security of its critical information infrastructure, China published 'Cybersecurity Review Measures' in 2020, outlining a set of rules to govern the review of supply-chain reliability and security underlying the products and services used by the operators of the infrastructure.[60] The government also released a draft Data Security Law in July 2020[61] and a draft Personal Information Protection Law in October 2020, representing the first comprehensive legislation relating to the security of personal data.[62]

Additionally, China's domestic cyber-security industry is much smaller than its US counterpart. Its total revenue in 2019, according to the Cybersecurity Association of China, was RMB 52.09bn (US$8.09bn),[63] which represented less than 7% of the global cyber-security industry (estimated at US$120bn in 2019).[64] The leading cyber-security firms in China have much lower revenues than those in the US, and much smaller global footprints. In the first quarter of 2020, for example, Cisco Systems, Palo Alto Networks and Fortinet respectively accounted for

9.1%, 7.8% and 5.9% of the global market[65] and the total US share was estimated at around 40%.[66]

China was ranked 27th out of 175 countries in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union (ITU).[67] Its ability to improve cyber security in the short to medium term will be constrained by its lack of a well-developed cyber-industrial complex – the enterprises, researchers and investors that help design and develop cyber-security technology. Cyber-security research and education in China is still at a basic level, with the country having no world-class universities in the field according to the Chinese University Alumni Association's 2019 ranking.[68]

Global leadership in cyberspace affairs

Since 2002, China has engaged in efforts through the UN, the ITU and other forums to establish new international governance and norms of behaviour for cyberspace, often leading like-minded states in arguing for greater censorship and state sovereignty.[69] It has worked closely in this process with Russia and other members of the Shanghai Cooperation Organisation. Since at least 2010, when then US secretary of state Hillary Clinton made a major speech on internet freedom,[70] China has found itself locked in an ideological battle with major Western states on the human-rights and security aspects of norm-setting for cyberspace.

On rare occasions China has joined an international consensus. In 2013, for example, its representative in the UN Group of Governmental Experts (GGE)[71] supported the collective agreement that international law applied in cyberspace, and in 2015 it joined a consensus position on possible voluntary norms for cyberspace. However, China subsequently took the view that the GGE process was not adequate for its purposes and became a leader in the push for an Open-Ended Working Group (OEWG), seen as a means of diluting Western influence and allowing unfiltered participation by all states in a UN-sponsored process.[72] The OEWG was created in 2018 and began operating a year later.

China's move away from the consensus position in the UN norms forums was mirrored on the global diplomatic stage by its leadership of an agenda on global internet governance much more in line with its interests. The first step, in 2014, was its creation of the Wuzhen Internet Forum, partly in response to a series of internet-governance conferences launched in London by the UK and like-minded countries in 2011. In March 2017 the Ministry of Foreign Affairs and the State Internet Information Office published China's vision in an 'International Strategy of Cooperation in Cyberspace', stating that the 'existing global governance system of basic internet resources hardly reflects the desires and interests of the majority of countries'.[73] Central to the document was the concept of 'cyber sovereignty': while Beijing has yet to define the term explicitly, it encompasses the idea that a state should have control over networks and content within its own borders.[74] Also, in September 2020, China moved assertively to propose a 'Global Data Security Initiative' during a high-level international symposium in Beijing, in direct opposition to the United States' Clean Network programme announced a month earlier.[75] Besides advocating a 'comprehensive and objective' approach towards data-security issues, the initiative also demands respect for the 'sovereignty, jurisdiction and security management rights' of other countries, aligning with China's concept of cyber sovereignty.[76]

Domestically, Beijing has passed legislation to compel foreign companies in China to store data on domestic servers and hand over sensitive intellectual property (IP) and source code for verification and testing – examples include the State Security Law (2015) and Cybersecurity Law (2017). Other laws, for example the National Encryption Law of 2019, have further asserted China's national-security interests in terms of its control of information technologies.[77] Such regulations present obvious risks of intellectual-property theft but also exemplify the type of norms and behaviours Beijing is increasingly promoting in international forums. China is pushing for reform of international institutions such as the UN Internet Governance Forum (IGF),[78] aiming to strengthen their decision-making capacity. Beijing sees UN rule-making in cyberspace as embodying the state-led approach to cyber governance, which it favours, rather than the West's vision of relatively unrestricted information flows.[79]

The normative effect of China's cyber-governance model is becoming increasingly apparent in other

authoritarian states, such as Vietnam and Russia, which have passed strikingly similar laws on internet regulation. Beijing has enabled oppressive politics in other states through the export of surveillance technology, in which China is now an industry leader. Huawei, for example, has worked with the security forces in Zimbabwe to build voice- and facial-recognition systems, and is also widely exporting its 'smart cities' technology, whose combination of bulk data collection, storage and AI-enabled surveillance offers governments a greatly increased capacity for surveillance and social control.

Beijing has advanced its cyber interests through the Digital Silk Road, a sub-strand of the BRI. This is a geo-economic initiative aiming to place China at the centre of a global digital supply chain dominated by Chinese digital goods and services, and held together by Chinese infrastructure, technological standards, laws and regulations. Though the initiative is still in its early stages, Chinese telecoms firms already provide products and services that sit at the core of telecoms infrastructure in many countries.

Chinese IT companies enjoy significant state backing in the form of subsidies and R&D inputs, and some of them, in particular Huawei, now enjoy global leadership in 5G technology alongside Western corporations. The potential for Chinese firms to provide 5G technology to networks across the world has met with fierce resistance from some Western states, whose political elites fear the security implications of Chinese technology and its potential to be used for espionage or disruption.[80] By mid-2020 the campaign against Huawei had significantly damaged its business prospects in major developed countries but had not achieved the same impact in most other states, nor prevented the company from making a profit overall.

Beijing has passed legislation to compel foreign companies in China to store data on domestic servers

China now plays a powerful role in global standard-setting in emerging technologies such as the Internet of Things, Internet Protocol Version 6 (IPv6) and 5G, and Beijing has attained key positions in international standard-setting agencies such as the International Organisation for Standardisation, the International Electrotechnical Commission and the ITU.[81] However, Western and allied countries continue to exert a strong influence in this arena through their world-leading corporations. Of the 51 tech or telecoms companies in the 2020 *Fortune* 'Global 500', China had only eight; the US and its allies or close partners had the other 43.[82]

Offensive cyber capability

China, like Russia, has made extensive use of lower-end cyber capabilities for peacetime influence-and-information operations, and thereby gained considerable experience of the relevant techniques. Based on published doctrine and proven cyber-intelligence reach, it is likely that China has also developed effective offensive cyber tools for combat use.

Though China has not published a cyber-warfare doctrine, and it may be the case that none exists,[83] authoritative PLA writings acknowledge the existence of an offensive cyber capability. The 2013 edition of *The Science of Military Strategy*, for example, dedicates a section to conflict in cyberspace and divides operations into the four categories of reconnaissance, attack, defence and deterrence, the first two of which are offensive in nature.[84] Computer reconnaissance is the use of computers to identify, monitor and analyse enemy computer networks and systems. It aims to prepare the ground in peacetime for future military operations by identifying weaknesses in adversary systems. As the requirements for successful penetration of an adversary system for reconnaissance purposes are similar to those in a 'network strike', it is possible to switch from reconnaissance to attack at the appropriate moment.[85]

The Chinese view is that network strikes could potentially follow soon after the outbreak of a conflict and would serve to disable an adversary system.[86] *The Science of Military Strategy* asserts that civilian as well as military infrastructure is a potential target during conflict, partly as the former sustains the latter but also because network strikes against civilian targets are less likely to escalate the conflict.[87] The PLA

is also considering the use of more advanced capabilities such as 'integrated network electronic warfare', which would enable it to insert malicious algorithms into an adversary network even if a wire connection does not exist. For example, Dai Qingmin, a former head of the Fourth Department of the General Staff, wrote as early as 1999 about the potential to use wireless (radio-based) cyber attacks to intercept satellites' communications or gain control over their command-and-control systems.[88]

Chinese assertions about the role and efficacy of such cyber attacks by their armed forces remain untested, so their potential impact in an actual combat engagement or war is unknown. Nevertheless, the PLA and Chinese intelligence agencies have successfully penetrated US government and commercial networks on multiple occasions, deploying malware to steal classified information and intellectual property. During a conflict the PLA's offensive cyber forces could presumably deploy similar capabilities to try to cripple the critical systems of an adversary. The knowledge acquired through past operations may also have shed light on vulnerabilities that could be exploited during wartime.[89] The PLA has both the capability and the will to penetrate adversary systems for the purpose of intelligence collection and offensive operations.

Notes

1 This CCP body was known as the Small Leading Group on Informatisation and Cyber Security until 2018, when it was upgraded to the status of a CCP commission and renamed the Central Commission for Informatisation and Cyber Security (CCIC). This put it on a similar level to powerful entities such as the Central Military Commission. Its name in English is often shortened to the Central Cyberspace Affairs Commission (CCAC). The equivalent government body remains the Cyberspace Administration of China, which operates in part as the secretariat or office for the CCIC.

2 Cyberspace Administration of China, 'National Cyberspace Security Strategy', 2016, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy.

3 Rogier Creemers, Paul Triolo and Graham Webster, 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)', New America, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china.

4 For an overview, see Greg Austin, *Cybersecurity in China: The Next Wave* (New York: Springer, 2018), p. 8.

5 China Internet Network Information Center, 'Statistical Report on Internet Development in China', August 2019, pp. 72–3, https://cnnic.com.cn/IDR/ReportDownloads/201911/P020191112539794960687.pdf. The report covers the first six months of 2019.

6 *Ibid*., p. 74.

7 See Greg Austin and Wenze Lu, 'Five Years of Cyber Security Education Reform in China', in Greg Austin (ed.), *Cyber Security Education: Principles and Policies* (Abingdon: Routledge, 2020).

8 For an overview of the early military developments, see Greg Austin, 'China's Security in the Information Age', in Lowell Dittmer and Maochun Yu (eds), *Routledge Handbook of Chinese Security* (Abingdon: Routledge, 2015), pp. 355–70.

9 Yan Weifeng, *Cong Meijun 'konghai yiti zhan' gouxiang kan zhanyi fazhan* (Beijing: Haichao Press, 2016), p. 197.

10 Parallel concepts employed by the PLA also include 'network space' (*wangluo kongjian*) instead of 'cyberspace', and 'network warfare' (*wangluo zhan*) instead of 'cyber operations'. The PLA's dictionary of military terms defines network warfare as 'operations to destroy an enemy's network systems and network information, [and] degrade their effectiveness, while protecting one's own network systems and network information'. See Military Terminology Committee, Academy of Military Sciences, *Military Terminology of the People's Liberation Army* (Beijing: AMS Publishing, 2011), p. 286.

11 Dean Cheng, 'Winning Without Fighting: The Chinese Psychological Warfare Challenge', The Heritage Foundation, 12 July 2013, p. 2, https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge/#_ftn1.

12 Jeffrey Engstrom, 'Systems Confrontation and Systems Destruction Warfare: How the People's Liberation Army Seeks to Wage Modern Warfare', RAND Corporation, 2018, p. 10, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1708/RAND_RR1708.pdf.

13 China Aerospace Studies Institute, *In Their Own Words: Foreign Military Thought – Science of Military Strategy 2013*, 8 February 2021, pp. 58, 160–1, 221, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf?ver=NxAWg4BPw_NylEjxaha8Aw%3d%3d.

14 State Council Information Office of the People's Republic of China, 'China's Military Strategy', May 2015, http://eng.mod.gov.cn/Database/WhitePapers/2014.htm.

15 See, for example, 'Réngōng zhìnéng jūnbèi jìngsài zhèngzài qiǎorán xīngqǐ', *China Youth Daily*, 17 October 2019, https://m.chinanews.com/wap/detail/zw/gn/2019/10-17/8981224.shtml.

16 'Xi calls for building a strong army', Xinhua, 26 October 2017, http://www.xinhuanet.com//english/2017-10/26/c_136708142.htm.

17 See Greg Austin, 'The Strategic Implications of China's Weak Cyber Defences', *Survival: Global Politics and Strategy*, vol. 62, no. 5, September–October 2020, pp. 119–38.

18 John Costello and Joe McReynolds, 'China's Strategic Support Force: A Force for a New Era', *China Strategic Perspectives*, Institute for National Strategic Studies, National Defense University, 2018, p. 5, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

19 *The Science of Military Strategy*, produced by the PLA's Academy of Military Science, terms this development 'integrated reconnaissance, attack, and defense' [*zhen gongfang yitihua*]. See Costello and McReynolds, 'China's Strategic Support Force: A Force for a New Era', p. 12.

20 *Ibid.*, p. 40.

21 *Ibid.*, pp. 40–1.

22 'Zhànlüè zhīyuán bùduì jīcéng jiànshè gōngzuò shùpíng', Xinhuanet, 24 September 2017, http://www.xinhuanet.com/mil/2017-09/27/c_129713342.htm.

23 MSS is the main civilian intelligence and counter-intelligence agency.

24 See endnote 1.

25 Brendon Hong, 'The American Money Behind Blacklisted Chinese AI Companies', Daily Beast, 2 January 2021, https://www.thedailybeast.com/the-american-money-behind-blacklisted-chinese-artificial-intelligence-companies.

26 Josh Rudolph, 'Sharper Eyes: Surveilling the Surveillers (Part 1)', *China Digital Times*, 9 September 2019, https://chinadigitaltimes.net/2019/09/sharper-eyes-surveilling-the-surveillers-part-1.

27 Nicholas Eftimiades, *Chinese Intelligence Operations* (Abingdon: Routledge, 2017).

28 See Greg Austin, *Cyber Policy in China* (Cambridge: Polity, 2014), p. 1.

29 China Academy of Information and Communications Technology, 'Zhōngguó shùzì jīngjì fāzhǎn báipíshū', May–July 2020, pp. 49–50, http://www.caict.ac.cn/kxyj/qwfb/bps/202007/P020200703318256637020.pdf.

30 Tahsin Saadi Sedik, 'Asia's Digital Revolution', *Finance & Development*, vol. 55, no. 3, September 2018, https://www.imf.org/external/pubs/ft/fandd/2018/09/asia-digital-revolution-sedik.htm.

31 China Academy of Information and Communications Technology, 'Zhōngguó shùzì jīngjì fāzhǎn báipíshū', p. 8.

32 *Ibid.*, p. 27. Alibaba ranked 132nd in the 2020 *Fortune* Global 500 and Tencent 197th.

33 Shannon Tiezzi, 'New Report Highlights China's Cybersecurity Nightmare', *Diplomat*, 18 February 2015, https://thediplomat.com/2015/02/new-report-highlights-chinas-cybersecurity-nightmare.

34 Davey Winder, 'China Prepares to Drop Microsoft Windows, Blames US Hacking Threat', *Forbes*, 30 May 2019, https://www.forbes.com/sites/daveywinder/2019/05/30/china-prepares-to-drop-microsoft-windows-blames-u-s-hacking-threat/?sh=doa00282c50d.

35 State Council of the People's Republic of China, 'Notice of the State Council Issuing the New Generation of Artificial Intelligence Development Plan', State Council Document no. 35, 8 July 2017, https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf.

36 Matt Ho, 'China's Hi-Tech Direction for the next Five Years', *South China Morning Post*, 11 November 2020, https://www.scmp.com/news/china/politics/article/3109316/chinas-hi-tech-direction-next-five-years.

37 Jeffrey Ding, 'China's Current Capabilities, Policies and Industrial Ecosystem in AI – Testimony before the U.S.–China Economic and Security Review Commission Hearing on Technology, Trade, and Military–Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy', US–China Economic and Security Review Commission,

7 June 2019, p. 4, https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Jeffrey%20Ding_China's%20Current%20Capabilities,%20Policies,%20and%20Industrial%20Ecosystem%20in%20AI.pdf.

38 *Ibid*., p. 40.

39 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.

40 Priyankar Bhunia, 'World's longest unhackable communications link opened between Beijing and Shanghai', OpenGovAsia, 28 October 2017, https://opengovasia.com/worlds-longest-unhackable-communications-link-opened-between-beijing-and-shanghai.

41 Liu Zhen, 'China's experiment in quantum communication brings Beijing closer to creating a hack-proof network', *South China Morning Post*, 9 January 2021, https://www.scmp.com/news/china/science/article/3117005/chinas-experiment-quantum-communication-brings-beijing-closer.

42 Union of Concerned Scientists, 'UCS Satellite Database', updated 1 January 2021, https://www.ucsusa.org/resources/satellite-database.

43 IISS, *The Military Balance 2021* (Abingdon: Routledge for the IISS, 2021), pp. 48, 191, 250.

44 Defence Intelligence Agency, 'Challenges to Security in Space', January 2019, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

45 Andrew Tate, 'China integrates long-range surveillance capabilities', *Jane's Intelligence Review*, vol. 29, no. 12, December 2017. See also Timothy Heath, 'China's Pursuit of Overseas Security', RAND Corporation, 2018, p. 30, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2271/RAND_RR2271.pdf.

46 'Haiyang-2 (HY-2 or Ocean-2)', Globalsecurity.org, https://www.globalsecurity.org/space/world/china/hy-2.htm.

47 Kevin L. Pollpeter, Michael S. Chase and Eric Heginbotham, 'The Creation of the PLA Strategic Support Force and its Implications for Chinese Military Space Operations', RAND Corporation, 2017, p. 7, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2058/RAND_RR2058.pdf.

48 Semiconductor Industry Association, '2020 – State of the U.S. Semiconductor Industry', p. 8, https://www.semiconductors.org/wp-content/uploads/2020/07/2020-SIA-State-of-the-Industry-Report-FINAL-1.pdf.

49 'China's Xi Jinping warns of new "long march" as trade war with US intensifies', *Straits Times*, 22 May 2019, https://www.straitstimes.com/asia/east-asia/chinese-president-xi-jinping-warns-of-new-long-march-as-trade-war-intensifies.

50 Elliott Zaagman, 'Cyber Sovereignty and the PRC's Vision for Global Internet Governance', *China Brief*, vol. 18, no. 10, 5 June 2018, https://jamestown.org/program/cyber-sovereignty-and-the-prcs-vision-for-global-internet-governance.

51 Roger Faligot, *Chinese Spies: From Chairman Mao to Xi Jinping* (Melbourne: Scribe, 2019), p. 395.

52 China National Computer Network Emergency Response Team, '2016 Nián wǒguó hùliánwǎng wǎngluò ānquán tàishì zòngshù', National Computer Network Emergency Technology Processing Coordination Center, April 2017, pp. 14–20, http://www.cac.gov.cn/wxb_pdf/CNCERT2017/2016situation.pdf.

53 *Ibid*., p. 15.

54 China Internet Network Information Center, 'Statistical Report on Internet Development in China', September 2020, p. 69, https://cnnic.com.cn/IDR/ReportDownloads/202012/P020201201530023411644.pdf.

55 *Ibid*., pp. 70–2.

56 *Ibid*., p. 73.

57 Samm Sacks and Robert O'Brien, 'What to Make of the Newly Established Cybersecurity Association of China', Center for Strategic and International Studies, 25 May 2016, https://www.csis.org/analysis/what-make-newly-established-cybersecurity-association-china.

58 Samm Sacks and Manyi Kathy Li, 'How Chinese Cybersecurity Standards Impact Doing Business in China', CSIS, 2 August 2018, https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

59 Dora Wang, Charmian Aw and Cindy Shen, 'MLPS 2.0: China's Enhanced Data Security Multi-Level Protection Scheme and Related Enforcement Updates', ReedSmith, 9 October 2019, https://www.reedsmith.com/en/perspectives/2019/10/mlps-20-chinas-enhanced-data-security-multi-level-protection.

60 Lauren Dudley et al., 'China's Cybersecurity Reviews Eye "Supply Chain Security" in "Critical" Industries [Translation]', New America, 27 April 2020, http://newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-eye-supply-chain-security-critical-industries-translation.

61 Emma Rafaelof et al., 'Translation: China's Data Security Law (Draft)', New America, 2 July 2020, http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft.

62 Bryan Cave, 'China's Draft Personal Information Protection Law: What Businesses Should Know', Lexology, 2 December 2020, https://www.lexology.com/library/detail.aspx?g=f7f7b85c-545a-4fbe-a114-833044603750.

63 Cybersecurity Association of China (CAICT), '2020 Nián zhōngguó wǎngluò ānquán chǎnyè tǒngjì bàogà', p. 8, https://www.cybersac.cn/News/getNewsDetail/id/1545. The estimate of RMB 52.309bn is for the annual revenue from technology products and services in cyber security for companies whose revenue arising from that sector is at least 50% of their total revenue. This report includes the data from around 500 cyber-security companies in China and can be regarded as a reliable estimate compatible with similar estimates made in previous years for the sector as a whole. The CAICT has published a much higher estimate but that includes many products and services not normally included in the cyber-security sector.

64 See Gartner, 'Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020', 17 June 2020, https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem.

65 Statista, 'Leading cybersecurity vendors by market share worldwide from 2017 to 2020', 2 July 2020, https://www.statista.com/statistics/991308/worldwide-cybersecurity-top-companies-by-market-share.

66 *Ibid*.

67 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 63, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

68 See Austin and Lu, 'Five Years of Cyber Security Education Reform in China'.

69 An overview of China's participation in debates on global norms for cyberspace can be found in Greg Austin, 'International legal norms in cyberspace: Evolution of China's national security motivations', in Anna Maria Osula and Henry Roigas (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (Tallinn: NATO CCDCOE Publications, 2016), pp. 172–201.

70 US Department of State, 'Remarks on Internet Freedom', Hillary Rodham Clinton, Secretary of State, Washington DC, 21 January 2010, https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

71 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.

72 United Nations General Assembly, 'Resolutions adopted by the General Assembly on 5 December 2018: Developments in the field of information and telecommunications in the context of international security', Resolution 73/27, 11 December 2018, https://undocs.org/en/A/RES/73/27. The OEWG's full name is the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. For details on its activities, see United Nations Office for Disarmament Affairs, 'Open-ended Working Group', https://www.un.org/disarmament/open-ended-working-group.

73 Tai Ming Cheung, 'The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities', *Journal of Cyber Policy*, vol. 3, no. 3, 2018, p. 313.

74 Zaagman, 'Cyber Sovereignty and the PRC's Vision for Global Internet Governance'.

75 Chun Han Wong, 'China Launches Initiative to Set Global Data-Security Rules', *Wall Street Journal*, 8 September 2020, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974.

76 China Ministry of Foreign Affairs, 'Quánqiú shùjù ānquán chàngyì', 8 September 2020, https://www.fmprc.gov.cn/web/wjbzhd/t1812949.shtml.

77 See National People's Congress of the People's Republic of China, 'Zhōnghuá rénmín gònghéguó mìmǎ fǎ (2019 nián 10 yuè 26 rì dì shísān jiè quánguó rénmín dàibiǎo dàhuì chángwù wěiyuánhuì dì shísì cì huìyì tōngguò'), 26 October 2019, http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml.

78 The IGF is a multi-stakeholder discussion forum set up in 2006 in the framework of the World Summit for the Information Society, a UN body left in place after related summits in 2002 and 2003. See 'The Internet Governance Forum (IGF)', UN Internet Governance Forum, 24 June 2015, https://www.intgovforum.org/cms/2015/IGF.24.06.2015.pdf.

79 Adam Segal, 'When China Rules the Web: Technology in Service of the State', *Foreign Affairs*, vol. 7, no. 5, September–October

2018, pp. 10–14, 16–18, https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web.

80 Nigel Inkster, *China's Cyber Power*, *Adelphi* 456 (Abingdon: Routledge for the IISS, 2015).

81 Kristin Shi-Kupfer and Mareike Ohlberg, 'China's Digital Rise: Challenges for Europe', MERICS Papers on China, no. 7, April 2019, p. 21, https://merics.org/sites/default/files/2020-06/MPOC_No.7_ChinasDigitalRise_web_final_2.pdf.

82 For the tech companies in the 2020 *Fortune* Global 500 ranking, see 'Global 500', *Fortune*, https://fortune.com/global500/2020/search/?sector=Technology. For the telecoms companies, see 'Global 500', *Fortune*, https://fortune.com/global500/2020/search/?sector=Telecommunications.

83 Kevin Pollpeter, 'Chinese Writings on Cyberwarfare and Coercion', in Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (eds), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press, 2015).

84 Amy Chang, 'Warring State: China's Cybersecurity Strategy', Center for a New American Security, December 2014, p. 25, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_WarringState_Chang_report_010615.pdf?mtime=20160906082142&focal=none.

85 Joe McReynolds, 'China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy', *China Brief*, vol. 15, no. 8, April 2015, p. 5, https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfare-lessons-from-the-science-of-military-strategy.

86 Pollpeter, 'Chinese Writings on Cyberwarfare and Coercion', p. 7.

87 McReynolds, 'China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy', p. 5.

88 Pollpeter, 'Chinese Writings on Cyberwarfare and Coercion', p. 8.

89 *Ibid.*, pp. 13–14.

9. Russia

Russia's cyber strategy is dictated by its confrontation with the West, in which it sees cyber operations as an essential component of a wider information war. Its cyber governance is centralised, hierarchical and under the president's personal control. The country is highly dependent on foreign ICT corporations and has a less impressive digital economy than, for example, the United Kingdom or France. It is seeking to redress key weaknesses in its cyber security through government regulation and the creation of a sovereign internet, and by encouraging the development of an indigenous digital industry. Given its economic circumstances, these ambitions may prove unrealistic. For two decades Russia has led, with some successes, diplomatic efforts to curtail what it sees as the dominance of cyberspace by the West, and particularly the United States. It has credible offensive cyber capabilities and has used them extensively as part of a much broader strategy aimed at disrupting the policies and politics of perceived adversaries, especially the US. It has run extensive cyber-intelligence operations, some of which reveal increasing levels of technical sophistication. However, Russia appears not to have given priority to developing the top-end surgical cyber capabilities needed for high-intensity warfare. Overall, Russia is a second-tier cyber power. To join the US in the first tier it would need to substantially improve its cyber security, increase its share of the global digital market and probably make further progress in developing the most sophisticated offensive military cyber tools.

Strategy and doctrine

Russian strategy and doctrine see cyber security and cyber operations as components of an information confrontation with the West. Russian sources refer more often to 'information space' than to 'cyberspace' and are doctrinally hardwired to integrate technical cyber operations with other means of achieving information superiority (for example by manipulating social media). In the last ten years Russia has sought to use such information capabilities to achieve strategic effect against its adversaries, a policy articulated to some extent in the concept of a 'grey zone' between peace and war mentioned in a magazine article by the Chief of the General Staff (CGS), Valery Gerasimov, in 2013.[1] There was evidence of these approaches in the Russian information operations against Estonia (2007), Georgia (2008) and Ukraine (2014–15), each of which had a component that Western observers described as 'cyber attacks'. But perhaps the most notorious example was the Russian 'hack and leak' operation against the Democratic National Committee during the presidential-election campaign in the United States in 2016.

List of acronyms

FSB	Federal Security Service
FSTEK	Federal Service for Technical and Export Control
GRU	Main Intelligence Directorate
ICT	information and communications technology
KGB	Committee of State Security
SORM	operational investigative-measures system
SVR	External Intelligence Service

This thinking was brought together in Russia's Information Security Doctrine of December 2016,[2] which, like the National Security Strategy of 2015, portrayed the country as under constant information attack.[3] The 2016 doctrine was similar in many respects to its equivalents in the other countries studied in this report. It covered strategic deterrence; the information security of government agencies, the armed forces, critical national infrastructure and citizens; and countering the threats posed by adversary states, terrorists and criminals. The main differences lay in the lack of any real distinction between military and civil-sector information security, and the focus on countering 'information' and 'psychological actions' aimed at undermining Russia's 'history', 'patriotism' and 'traditional moral and spiritual values'. Russia's strategy seems to put special emphasis on controlling the information and content available on its networks, which the authorities clearly see as a primary threat. This is consistent with the Russian view that cyber threats are a component of broader information campaigns being conducted by its adversaries, aimed at changing the fabric of Russian society. As a result, the 2016 doctrine advocated an increased role for Russia's own internet management and greater domestic production of information technology. Interestingly, it also described how, in the interests of national security, Russia would be able to counter its adversaries by employing its own information campaigns against them. All subsequent government documents on information security have made numerous references to the 2016 doctrine.

The Information Security Doctrine of 2016 also drew heavily on earlier Russian military concepts for the use of cyberspace, encapsulated in a Ministry of Defence publication from 2011,[4] and in the Military Doctrine of 2014.[5] The 2011 publication provided an indication of how the Russian armed forces saw their role in cyberspace but it appeared incomplete, focusing on situational and threat awareness, and on force protection, while making no mention of offensive cyber or information operations. Its preamble included an official statement on the threat to Russia's information security posed by other states' development of information-warfare policies – further evidence of a conspiratorial view of the world in which hostile intent is assumed to lie behind all online activities emanating from the West.[6]

The 2014 Military Doctrine was notable for its recognition that modern warfare would involve a highly novel integration of 'military force and political, economic, informational or other non-military measures implemented with a wide use of the protest potential of the population and of special operations forces'.[7] It placed information risks 12th in a list of external threats, but first in its list of internal ones. In its list of the ten main features of modern warfare, the first three were information-related. And in its long list of main tasks necessary in order to deter and prevent an armed attack against Russia, information operations were placed first.

In 2017, after a long period in development, Russia announced that 'information-operations troops' were joining its armed forces.[8] These units were intended to fill a gap in capabilities that became apparent during the 2008 conflict in Georgia. Although the new formations have been perceived in the Western media as primarily providing a cyber capability, their role so far seems more in keeping with the broader Russian definition of information warfare. In exercises – and on deployment to Syria – they have in some cases used traditional psychological-operations techniques such as leaflet drops and loudspeaker broadcasts in foreign languages.[9] They are also equipped with systems for interference with civilian mobile-phone communications, including broadcasting content to them. These electronic capabilities have been used for disinformation, demoralisation and propaganda purposes in Syria and Ukraine, and against NATO personnel in the Baltic states.[10]

Russia's traditional lack of military digitisation (compared, for example, with the US) has begun to be redressed, both at tactical level and at the level of national command and control. There is a recognition that new organisations and new leadership dispositions will be necessary to enable Russia to compete with the US and its allies, and that this will require a whole-of-society approach supported by networked and integrated communications. Though Russia has produced very little in the way of formal documents for military strategic planning for cyberspace since 2017, the subject is a highly topical one. CGS Gerasimov observed in a

2020 briefing to military attachés that strategic confrontation in cyberspace is intensifying and that there is a risk of it interfering with the command and control of strategic nuclear systems.[11] A year earlier, another military commentary stated that dominance in cyberspace (alongside military power) is a precondition for victory in modern war.[12] Specialist military commentaries have continued to focus as much on the cognitive and psychological aspects of cyber conflict as on the other dimensions, and have shown a particular interest in China's information warfare.[13]

Governance, command and control

The president takes the lead on cyber-security governance and exercises national command and control of key agencies through the Security Council. Policy documents make reference to a multi-stakeholder approach to the management of national cyber security – in which business and community groups supposedly have input, alongside regional governments – but in reality the system is presidential and state-controlled. The secretary of the Security Council is mandated under the 2016 Information Security Doctrine to provide annual reports to the president on the state of the country's cyber security. There is an assigned lead officer for cyber-security policy within the Security Council, at deputy-secretary level. The leading cyber agencies are represented at higher levels within the Security Council: its permanent members include the defence minister and the head of the Federal Security Service (FSB),[14] and its other members include the Chief of the General Staff.[15]

Russia's traditional lack of military digitisation has begun to be redressed, both at tactical level and at the level of national command and control

In terms of the leadership and coordination of cyber policy and operations, President Vladimir Putin appears to give priority to the Ministry of Defence. For offensive operations, the Main Directorate of the General Staff (formerly the Main Intelligence Directorate or GRU) has primary responsibility. The 8th Directorate of the General Staff provides cryptographic services and supervises the management of military secrets relating to cyber affairs. The FSB, the country's main domestic intelligence agency, is tasked with defence against attacks on government systems and critical national infrastructure. It inherited the functions of earlier cyber and signals-intelligence agencies that were disbanded during President Putin's early years. In 2018 the FSB set up a National Coordination Centre for Computer Incidents, whose commander is also the director of the FSB's Centre for Data Protection and Special Communications.[16]

The Federal Service for Technical and Export Control (FSTEK),[17] part of the Ministry of Defence, is charged with certain roles in protecting critical information infrastructure across the country, taking the lead in defensive measures against any foreign technology-based intelligence operations, technical defence of information, and policy for export controls on technology.[18] One its most important duties is technical counter-intelligence operations inside Russia. FSTEK activities cover a wide range of policy, including the the regulations covering the use of foreign information technology.

At an early stage in the debate on new units dedicated to information operations, following the 2008 conflict in Georgia, the FSB appeared to publicly denounce plans by the armed forces to develop their own information-warfare capability, stating that such a capability should be the preserve of the FSB. The FSB's monopoly has since been eroded, however, judging by evidence of the role of the Russian military-intelligence service in information-warfare activities globally and by the assignment to FSTEK in 2017 of key cyber-defence-policy responsibilities involving national politics and the economy.

The National Defence Management Centre in Moscow is Russia's strategic command post, established in 2014 to operate around the clock as the country's first fusion hub for information and communications from all agencies. It is located close to the Kremlin and fulfils four functions: high command; coordination for military operations; command of strategic nuclear forces; and coordination of the peacetime work of the security

ministries and agencies, including cyber security.[19] By initially combining 49 military, police, economic, infrastructure and other authorities under the stewardship of the General Staff, the centre has improved the speed of government reaction and information exchange.[20] By 2020 it was involved in coordinating military exercises with much larger numbers of entities – in the *Kavkaz* 2020 exercise, for example, there were 160 participating entities and the centre coordinated 380 joint actions.[21]

Core cyber-intelligence capability

After the collapse of the Soviet Union in 1991, its intelligence agencies were regrouped within the Russian Federation. The former Committee of State Security (KGB)[22] was split into two agencies, both of which had acquired their current names by 1995: the FSB,[23] which took over the KGB's internal-security functions, and the External Intelligence Service (SVR),[24] which took over its activities abroad. The role of the armed forces' Main Intelligence Directorate (GRU)[25] changed very little, though its name was shortened to Main Directorate (GU)[26] in 2010 (Putin later said that the word 'Intelligence' should have been maintained). The intelligence agencies enjoy the highest level of political support and supervision, with Putin relying on them for his domestic power in an authoritarian type of guided democracy. This has involved ruthless exploitation of the intelligence power of the state, manifested in assassinations of political opponents, both inside and outside Russia, and in Putin's personal authorisation of a campaign of political interference in the 2016 US presidential election.[27] Indeed, the nature and increasing volume of Russia's overseas intelligence activity suggests the country's security and intelligence agencies have inherited the KGB's doctrine of intelligence as a form of 'political struggle' and are in a permanent state of 'political war' against the West, albeit with adjustments to the realities of the twenty-first century.[28]

For the purposes of internal security the Russian state monitors online activity by using its operational investigative-measures system (SORM),[29] a well-documented set of regulations that controls Russian internet service providers (ISPs).[30] SORM provides Russian law-enforcement bodies with a wide range of cyber-surveillance material,[31] capturing meta-data and content from mobile and landline calls (SORM-1), internet traffic (SORM-2) and all other media (SORM-3). In theory, retrieval of intercepted data requires court orders, but in practice this is most likely ignored by the Russian security services.

As in China, the perceived misuse of social media is regarded as a significant national-security issue, with controls in place to prevent distribution of information hostile to the state. The powers of surveillance of the Russian state have been further enhanced by laws and measures ostensibly aimed at data protection and combating terrorism, with increasingly stringent rules requiring ISPs to collect and store data on user activity. This includes the capturing of user information for periods of between six months and three years – including all written, audio and video communications; home address; passport details; lists of relatives, friends and contacts; social-media accounts; languages spoken; and records of all e-payments.

As in China, the perceived misuse of social media is regarded as a significant national-security issue

Given the growing number of overseas cyber attacks that Western governments and companies have attributed to the GU and other Russian actors, and that some of those attacks appear to have been complex intelligence-gathering operations, it is safe to assume that Russia also possesses extensive regional and global cyber-intelligence capabilities.

As with other aspects of Russian intelligence operations, the tradecraft sometimes appears less sophisticated than that employed by Western cyber operators, but in such cases the Russians may care less than their foreign counterparts about getting caught. This even applies to the well-publicised and widespread Russian cyber-intelligence operations detected by the US at the end of 2020, which employed some sophisticated techniques to evade US private-sector cyber security but still made indiscriminate use of ubiquitous IT vulnerabilities. (The attack involved the hacking of software

supplied by the US company SolarWinds to a wide range of US government and private-sector clients.)[32] In comparison, a Russian intelligence operation in 2008 that penetrated US Department of Defense networks appeared to be much more carefully targeted.[33]

Russia has fewer financial resources to invest in intelligence capabilities than the US or China. One means of compensating for this, it seems, is to blur the dividing line between state and non-state actors.[34] The use of so-called 'patriotic hackers' and organised cyber-crime expertise is believed to substantially enhance Russia's cyber capabilities.[35] Since the attack by Russian hackers on Estonia in 2007, the Kremlin has sourced technology and even intelligence information from such groups operating within its near abroad. It is unclear precisely how much direction patriotic hackers and cyber criminals are given by the Kremlin, but often their activities have no discernible motive apart from furthering the aims of the Russian state.

Cyber empowerment and dependence

Russia's adoption of a digital economy has been gradual. According to the Russian Association of Electronic Communications (RAEC), internet-dependent industries account for up to 20% of GDP. However, the RAEC has also estimated that some of the onerous regulatory demands already introduced or set to be introduced, especially data-storage requirements contained in anti-terrorism laws passed in 2016, could hamper the further development of the digital economy. Russia is only a mid-level performer in digital competitiveness, demonstrated in part by it not having any of the 51 tech or telecoms companies that appeared in the 2020 *Fortune* 'Global 500', whereas the US had 16 and China eight.[36]

In 2017, President Putin issued a decree on the need for Russia to become an 'information society'.[37] A follow-on to a similar document in 2008, it highlighted the challenges the country was facing as it attempted to build a stronger digital economy. Its aims included an expansion of Russian encryption technologies; the replacement of foreign ICT equipment by domestically produced technologies (especially in critical information infrastructure); and improvements in the effectiveness of domestic communications networks to support a 'centralized system of monitoring and management of the Russian electronic grid'.[38]

The number of Russian internet users continues to rise, though the rate of growth has slowed. According to the 2020 edition of a large-scale survey carried out by Russia's Public Opinion Foundation, 69% of respondents had been online at some point in the preceding 24 hours.[39]

Smartphones are the most popular way for Russians to access the internet. Internet penetration in the metropolitan hubs of Moscow and St Petersburg is significantly above the national average – around 80% of adults, compared with about 60% in rural areas.[40] Prices are quite low by international standards, with the *Economist* putting the country in 12th position in its ranking of overall affordability of mobile and fixed-line internet charges.[41] In terms of 'readiness' (the population's 'capacity to access the Internet', taking into account skills, cultural acceptance and supporting policy) the *Economist* put Russia in 59th position.

The most dramatic and high-profile expression of Russia's focus on cyber empowerment and independence is its attempt to create a separate domestic internet – a concept it refers to as the 'sovereign RuNet'. The Kremlin's determination to significantly increase its control over the internet became clear soon after Putin returned to the Kremlin in 2012 for his third term as president. The use of social media to organise mass protests in Moscow in 2011 and an awareness of its role in the Arab Spring convinced the newly re-elected president and his supporters that the RuNet could no longer be left to its own devices. Two events reinforced this view and allowed the Kremlin to present its policy of internet control as an issue of national security: the 2013 leaks by US defector Edward Snowden, revealing the extent and nature of US cyber intelligence; and the 2013–14 Euromaidan protests in Ukraine, in which platforms such as Facebook again proved indispensable in allowing disparate protesters to join forces to oppose and ultimately overthrow the regime of pro-Russian president Victor Yanukovych.

Much of the internet legislation passed in Putin's third term (2012–18) was clearly linked to the pursuit of information sovereignty. One of the stated aims was to isolate the RuNet from the global internet. In 2016 the Communications Ministry set the goal of ensuring that 99% of internet traffic in the RuNet would be routed within Russia itself by 2020,[42] a target figure that

dropped to 90% within a year. It should be noted, however, that the ambition is not to regularly prevent internet traffic from leaving Russian servers but instead to provide the capability to insulate the country from international traffic (inwards and outwards) in the event of a crisis.[43] Russia's aim of becoming a digital economy and society would not be achieved if it enforced a lockdown of internet traffic for more than a couple of weeks. All international transactions in financial services are based on the internet, for example, as is the international exchange of information on health issues.

The Russian government claimed in December 2019 to have successfully tested the disconnection of the RuNet from the internet. It stated that several disconnection scenarios had been tested, including a simulation of a state-backed cyber attack and a response described as 'combat mode'.[44] The tests involved government agencies and telecoms companies, including local ISPs.

Russia is a self-sufficient space power, operating its own satellite-communications and satellite-navigation constellations, serving both civil and military purposes, as well as satellites for a range of other functions. Its satellite-navigation system, GLONASS (Global Navigation Satellite System), is equivalent to the US Global Positioning System (GPS) and its 24 operational satellites provide complete global coverage. In normal circumstances, each of these national systems can rely on others for enhanced accuracy. As of January 2021, Russia was operating 176 satellites while China had more than double that number (412) and the US more than ten times as many (1,897).[45]

Cyber security and resilience

Putin has made national cyber resilience and security a high priority during his two decades as leader of Russia, beginning in 2000 with the release of the first Information Security Doctrine, within months of his inauguration as president. In 2016 the government intensified its efforts, issuing a raft of new laws and reforms to address social and technical aspects of the challenge, along with an updated Information Security Doctrine. Key elements of this resilience policy have included the RuNet and the SORM surveillance regime.

Another element is a secure government network, RSNet, for the use of Russian government officials. All employees have their own secure work-email accounts that can only be accessed from a special IP address using a designated computer, but roll-out of the system is reportedly patchy.[56]

The government has also been pursuing other regulatory efforts, including a data-localisation law that requires corporations, including social-media platforms, to store Russian users' data within the country's borders.[46] For instance, Roskomnadzor, the federal body that oversees data compliance and censorship, has pushed Apple to store certain kinds of data in Russia rather than outside the country. In 2016 Russia blocked LinkedIn for non-compliance with the data-localisation law,[47] and in 2020 a Moscow court fined Twitter and Facebook US$63,000 each for non-compliance.[48] However, data localisation is generally very difficult for any country to enforce strictly.

A range of Computer Emergency Response Teams (CERTs) are nominally operational in Russia. They include both government and private-sector entities, such as CERT.GOV.RU, responsible for governmental networks; FinCERT for the Bank of Russia; Kaspersky ICS CERT for industrial control systems; and CERT-GIB.[49] A range of state research institutes and commercial companies are also involved in the work on cyber defences.

The government has also relied on public–private information-sharing arrangements, primarily through a system created in 2013 and known as GosSOPKA,[50] the 'state system for the detection, warning and liquidation of the consequences of computer attacks'. It aims to establish a constantly monitored perimeter to shield all government information resources within a single network.[51] The perimeter is intended to extend to all critical national infrastructure, with information on cyber attacks coordinated by a central body that would determine the nature of the attack and transmit appropriate security recommendations to the rest of the system. In early 2019 a Russian analyst assessed that the development of the system was still at an early stage.[52] The Republic of Tyva was the first Russian constituent entity to be connected to GosSOPKA, in 2019,[53] and the rules for the provision of subsidies for the creation of GosSOPKA 'industry' centres were also approved.[54] March 2020 saw the inauguration of a Security Code Monitoring and Response Centre that will contribute to the functioning of the system.[55]

In 2019 and 2020 the government took steps to make the use of intrusion-detection software compulsory in Russian IT systems, with FSTEK playing a key role. The FSB mandated that companies registered as 'information dissemination organisers' install equipment that would allow its intelligence officers constant decrypted access to user communications without the need for authorisation.[56] In December 2019 the government passed the Law on Software Pre-installation, requiring the downloading of Russian-made software into digital devices such as smartphones, computers and televisions entering the Russian market. A list of applications to be installed was approved, to take effect from 1 January 2021 (after an earlier date of entry into force was deferred because of the COVID-19 pandemic).[57] Once enforced, the new law means users face the possibility that their devices will contain surveillance apps and traffic-decryption certificates.[58] The government has also reportedly begun to step up efforts to apply deep packet inspection.[54] Russian cyber systems are now probably among the most regulated in the world. The aim is clear: to have a flexible, if complex, national cyber-defence system that might give Russia an advantage in a cyber conflict with another major power.[59] So far, however, there is little indication of whether these measures will be effective.

In the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union, Russia ranked 26th out of 175 countries.[60] Like most other countries, it is facing an escalation in successful cyber attacks. In 2020, for example, its online retailers saw a doubling of distributed-denial-of-service attacks[61] and the number of data-leak incidents in the financial-services sector grew by 36.5%.[62] In January 2021 the government issued a warning about possible US retaliatory cyber attacks on the country.[63] In February 2021 Putin addressed the board of the FSB, urging it to pay more attention to cyber security, among other threats, and noting that in 2020, 'if we take only those regarded as the most dangerous, the number of attacks on Russian websites, including government websites, surged by almost 350 percent'.[64] In March 2021 the president informed the Interior Ministry Board that the number of cyber crimes had increased more than tenfold during the previous six years.[65] According to the Russian business newspaper *Vedomosti*, more than half of the simulated cyber attacks carried out in 2019 were successful in penetrating the country's cyber defences.[66]

Global leadership in cyberspace affairs

Since 1998, Russia has sponsored an annual United Nations General Assembly resolution entitled 'Developments in the field of information and telecommunications in the context of international security', which expresses concern that malicious activity in cyberspace can undermine international peace and security. The resolution was initially uncontroversial, but early in the presidency of George W. Bush the US and its allies came to see it as a potential vehicle for promoting an authoritarian agenda on the part of Russia, China and like-minded states, aimed at limiting internet freedom. The resolution was used to create the UN Group of Governmental Experts (GGE)[67] process on cyber norms, beginning in 2002. Despite limited progress in reconciling the conflicting views of the opposing camps, GGE meetings have led to consensus reports on the applicability of international law to cyberspace on two occasions (2013 and 2015). These reports included acceptance of the applicability of international law to cyberspace, and recommendations on a set of norms, capacity-building and the importance of confidence-building measures.[68] Russia has been leading an international campaign aimed at establishing international agreements or treaties on information security, especially since tabling a Draft Convention on International Information Security in 2010. In 2020 it added a proposal for a non-intervention pledge regarding ICT-based attacks on the electoral process in other countries.[69]

The dialogue between Russia and Western states on cyberspace issues has been characterised by mutual incomprehension and apparent intransigence. Norms that one side takes for granted tend to be seen as threatening by the other. This divergence undermines attempts to reach agreement on common principles or rules of behaviour for cyberspace, despite Russia having repeatedly presented norms to which it invited other states to subscribe.

Russia cooperates quite closely with China in cyber diplomacy, especially through multilateral forums. This was evident in their joint leadership of the initiative to

set up the UN Open-Ended Working Group (OEWG) on cyberspace security in 2018,[70] which was open to all UN member states and aimed at countering the influence Western powers were exercising through the GGE. Russia is wary, however, about any operational collaboration with China on technical aspects of cyber policy.

Offensive cyber capability

Russia has developed its cyber capabilities and doctrine over more than two decades, successfully integrating them into its wider strategic thinking and its political agenda and goals. A characteristic of the Russian use of offensive cyber is a proven ability to integrate it fully into strategic information campaigns and into full-spectrum low-intensity state-on-state military operations. This could expose a weakness in any Western approach to cyber security that overly focuses on technical responses to technical threats while disregarding the interface with a broader campaign. For the Russians, such a campaign could see the seamless melding of disinformation, subversion, and kinetic-, cyber- and electronic-warfare operations to achieve highly ambitious aims, up to and including regime change in the target state.

The list of detected and attributed operations is a long one. It includes operations against the critical national infrastructure of states, such as denying access to critical communications media – examples include Estonia (2007), Georgia (2008), and Ukraine (2015). It includes interference in elections in the West, most notably the 2016 US presidential election. And it includes attempts to disrupt international investigations, for example into doping in sport, the shooting-down of Malaysia Airlines flight MH17 and the use of a chemical weapon in the United Kingdom. There has also been the disinformation campaign waged by the St Petersburg-based Internet Research Agency, nominally a private organisation, set up in 2013, that nevertheless has close links to President Putin. US authorities detected in 2016 that it was conducting disinformation and social-media operations during the US presidential-election campaign.

Russia employs a wide variety of techniques for such cyber operations, but all are based on some version of the classic cycle of reconnaissance, penetration, collection, analysis and action. These operations have included the leaking of hacked information into the public domain through online proxies, often deliberately amplified by Russian media outlets. The best-known example of this is the passing to WikiLeaks of emails hacked from the Democratic National Committee in the US in 2016. Other tactics include the aggressive deployment of teams into the field to gain access to the devices and systems of political opponents; jamming, controlling and inserting fake information into telecommunications networks; and the use of cyber criminals and so-called patriotic hackers. Russia has also become notorious for the ubiquitous use of trolls (online profiles run by humans) and bots (those run by automated processes) to plant, disseminate and lend credibility to disinformation by exploiting certain features of the relationship between traditional and social media.

Russia is today using offensive cyber capabilities extensively as part of a much broader strategy aimed at disrupting adversaries

Russia also appears to be exploring the potential deployment of other assets for strategic cyber effect in a time of crisis. It is reported, for example, to be contemplating the use of submarine assets to surveil or cut internet traffic between the US and Europe,[71] and the use of space vehicles to similarly degrade Western satellite-based communications.

It is likely that each of the three main Russian intelligence agencies (the FSB, GU/GRU and SVR) possesses, and uses, offensive cyber capabilities. For example, as well as having its own cyber specialists, the FSB reportedly recruits hackers to launch cyber attacks when it wants to punish or silence the Kremlin's rivals. But although the many exposures of its operations might not be the best indicator, the GU/GRU seems to have emerged as the main Russian proponent of offensive cyber operations. It hacked a French television station under the false flag of the Cyber Caliphate in 2015,[72] it was a main actor in the hack of the US Democratic National Committee in 2016, and it deployed the highly disruptive NotPetya computer virus against Ukraine

in 2017.[73] In 2020 the Security Service of Ukraine neutralised 103 Russian cyber attacks against websites of Ukrainian public authorities – the attacks had been intended to infiltrate information systems in order to modify or destroy data, or to delegitimise the Ukrainian authorities by spreading disinformation.[74] It is unknown whether the Russian cyber-intelligence operations that hacked software supplied by the US company SolarWinds to a wide range of US government and private-sector clients, discovered in late 2020, were conducted with any offensive-cyber purpose (it seems unlikely, but US investigations are ongoing).[75]

In summary, Russia is today using offensive cyber capabilities extensively as part of a much broader strategy aimed at disrupting and competing with perceived adversaries, especially the US. However, much of the detected tradecraft is relatively unsophisticated, and at times reckless, in comparison with the methods designed by the US and several of its allies for high-intensity warfare and/or surgical strategic effect. For example, there is no publicly known indication that Russia could match the capability used by the US and Israel in the 2008–10 Stuxnet operation against Iran. A possible indication that the Russians themselves suspect they are outmatched in this respect is their repeated attempts in international forums to make the military use of offensive cyber tools illegal under international law.

Notes

1 Valery Gerasimov, 'Tsennost' nauki v predvidenii', *Voenno-promyshlennyi kurier*, 27 February 2013, https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf. Translation available in Mark Galeotti, 'The "Gerasimov Doctrine" and Russian Non-Linear War', In Moscow's Shadows blog, 6 July 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war.

2 Presidential Administration, 'Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii', 6 December 2016, https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

3 Katri Pynnöniemi and Martti J. Kari. 'Russia's New Information Security Doctrine: Guarding a besieged cyber fortress', Finnish Institute of International Affairs, Comment no. 26/2016, December 2016, https://www.fiia.fi/wp-content/uploads/2017/04/comment26_russia_s_new_information_security_doctrine.pdf.

4 Ministry of Defence, 'Kontseptual'nye vzgliady na deiatel'nost' Vooruzhionnykh Sil Rossiiskoi Federatsii v informatsionnom prostranstve', 22 December 2011, http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

5 Office of the President, 'The Military Doctrine of the Russian Federation', 25 December 2014, https://rusemb.org.uk/press/2029.

6 See the chapter 'Russia under Threat' in Keir Giles, *Moscow Rules: What Drives Russia to Confront the West* (Washington DC: Brookings Institution Press, 2019), pp. 35–58.

7 Office of the President, 'The Military Doctrine of the Russian Federation'.

8 'V Minoborony RF sozdali voiska informatsionnykh operatsii', Interfax, 22 February 2017, http://www.interfax.ru/russia/551054.

9 See Mikhail Klikushin, 'Putin's Army Demands "NATO Soldiers! Hands Up! Lay Down Your Weapons!"', Observer.com, 19 August 2016, http://observer.com/2016/08/putins-army-demands-nato-soldiers-hands-up-lay-down-your-weapons.

10 Keir Giles, 'Assessing Russia's Reorganized and Rearmed Military', Carnegie Endowment for International Peace, May 2017, https://carnegieendowment.org/2017/05/03/assessing-russia-s-reorganized-and-rearmed-military-pub-69853. For instances of the use of similar techniques, see Dasha Zubkova, 'Defense Ministry: Russia Sending SMS Messages Asking Residents of Ukrainian Border Regions to Appear at Nearest Military Units', Ukrainian News, 27 November 2018, https://ukranews.com/en/news/598565-defense-ministry-russia-sending-sms-messages-asking-residents-of-ukrainian-border-regions-to-appear.

11 Ministry of Defence, 'Nachal'nik General'nogo shtaba VS RF general armii Valeriy Gerasimov provel brifing dlya inostrannykh

voyennykh attashe', 24 December 2020, https://function.mil.ru/news_page/country/more.htm?id=12331668@egNews.

12 Ministry of Defence, 'Prevoskhodstvo v kiberprostranstve stanovitsya odnim iz usloviy pobedy v voynakh', 22 April 2019, https://function.mil.ru/news_page/country/more.htm?id=12227079@egNews.

13 This observation is based on a review of the contents in two key journals, *Voennaia mysl'* and *Informatsionnye voiny*, from 2017 to 2021. A possible explanation of the lack of attention to the technical aspects is that in Russia there is much less public information on those subjects.

14 Federal'naia sluzhba bezopasnosti

15 See President of Russia, 'Security Council structure', http://en.kremlin.ru/structure/security-council/members.

16 'Russian domestic security service launch new dedicated center to counter cyberattacks', Russia Today, 11 September 2018, https://www.rt.com/russia/438142-russian-security-cyber-attacks.

17 Federal'naia sluzhba po tekhnicheskomu i eksportnomu kontroliu

18 Responsibility for key missions was assigned to FSTEK in Decree no. 569 of 25 November 2017, 'Ukaz Prezidenta RF ot 25 noiabria 2017 g. N 569 "O vnesenii izmenenii v Polozhenie o Federal'noi sluzhbe po tekhnicheskomu i eksportnomu kontroliu, utverzhdennoe Ukazom Prezidenta Rossiyskoi Federatsii ot 16 avgusta 2004 g. N 1085"', http://ivo.garant.ru/#/document/71818302/paragraph/1:0.

19 Roger McDermott, 'Russia Activates New Defense Management Center', Eurasia Daily Monitor, vol. 11, no. 196, 2 November 2014, https://jamestown.org/program/russia-activates-new-defense-management-center.

20 Keir Giles, 'Russia's "New" Tools for Confronting the West – Continuity and Innovation in Moscow's Exercise of Power', Russia and Eurasia Programme, Chatham House, March 2016, p. 25, https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.

21 Ministry of Defence, 'Nachal'nik NTsUO general-polkovnik Mikhail Mizintsev vystupil s dokladom na konferentsii "Razvitiye sistemy mezhvedomstvennogo vzaimodeystviya v oblasti oborony v 2020 godu"', 20 November 2020, https://function.mil.ru/news_page/country/more.htm?id=12325783@egNews.

22 Komitet gosudarstvennoi bezopasnosti

23 The FSB has 'authority to implement government policy in the national security of the Russian Federation, counterterrorism, the protection and defence of the state border of the Russian Federation, the protection of internal sea waters, the territorial sea, the exclusive economic zone, the continental shelf and their natural resources, ensuring the information security of Russia and exercising the basic functions of the federal security services specified in the Russian legislation, as well as coordinating the counterintelligence efforts of the federal executive bodies'. See Russian Government, 'Federal Security Service', http://government.ru/en/department/113.

24 Sluzhba vneshnei razvedki

25 Glavnoe razvedyvatel'noe upravlenie

26 Glavnoe upravlenie

27 United States Office of the Director of National Intelligence, 'Assessing Russian Activities and Intentions in Recent US Elections', 6 January 2017, p. ii, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

28 Mark Galeotti, 'Russian intelligence is at (political) war', *NATO Review*, May 2017, https://www.nato.int/docu/review/2017/also-in-2017/russian-intelligence-political-war-security/en/index.htm.

29 Sistema operativno-razysknykh meropriiatii

30 Keir Giles and Kim Hartmann, 'Socio-Political Effects of Active Cyber Defence Measures', in P. Brangetto, M. Maybaum and J. Stinissen (eds), *6th International Conference on Cyber Conflict, Proceedings* (Tallinn: NATO CCDCOE Publications, 2014), https://www.ccdcoe.org/uploads/2018/10/doroso_giles.pdf.

31 *Ibid*.

32 David E. Sanger, Nicole Perlroth and Julian E. Barnes, 'As Understanding of Russian Hacking Grows, So Does Alarm', *New York Times*, 2 January 2021, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

33 Ellen Nakashima, 'Cyber Intruder Sparks Response, Debate', *Washington Post*, 8 December 2011, https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

34 Andrew Foxall, 'Putin's Cyberwar: Russia's Statecraft in the Fifth Domain', Russia Studies Centre Policy Paper no. 9 (2016), The Henry Jackson Society, May 2016, https://www.stratcomcoe.org/afoxall-putins-cyberwar-russias-statecraft-fifth-domain.

35 Cory Bennett, 'Kremlin's ties to Russian cyber gangs sow US concerns', *Hill*, 11 October 2015, http://thehill.com/policy/cybersecurity/256573-kremlins-ties-russian-cyber-gangs-sow-us-concerns.

36 For the tech companies in the 2020 *Fortune* Global 500 ranking, see 'Global 500', *Fortune*, https://fortune.com/global500/2020/

search/?sector=Technology. For the telecoms companies, see 'Global 500', *Fortune*, https://fortune.com/global500/2020/search/?sector=Telecommunications.

37 Office of the President, 'Ukaz Prezidenta Rossiiskoi Federatsii o Strategii po razvitii informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017–2030 gody', 10 May 2017, http://publication.pravo.gov.ru/Document/View/0001201705100002?index=0&rangeSize=1.

38 Sergey Sukhankin, 'Russia Adopts New Strategy for Development of Information Society', *Eurasia Daily Monitor*, vol. 14, no. 66, 16 May 2017, https://jamestown.org/program/russia-adopts-new-strategy-development-information-society.

39 Fond obshchestvennoe mnenie, 'Internet i onlain servisy', 31 March 2020, https://fom.ru/SMI-i-internet/14402.

40 *Ibid.*

41 'The Inclusive Internet Index 2020', Economist Intelligence Unit, https://theinclusiveinternet.eiu.com/explore/countries/performance?category=affordability.

42 'Russia's Communications Ministry plans to isolate the RuNet by 2020', *Vedomosti*, 13 May 2016, carried by meduza.io, https://meduza.io/en/news/2016/05/13/communications-ministry-plans-to-isolate-runet-by-2020.

43 See Juha Kukkola, 'The Russian Segment of the Internet as a Resilient Battlefield', in Juha Kukkola, Mari Ristolainen and Juha-Pekka Nikkarila (eds), *GAME PLAYER: Facing the structural transformation of cyberspace* (Helsinki: Finnish Defence Research Agency, 2019), pp. 117–32, https://maanpuolustuskorkeakoulu.fi/documents/1948673/10330463/PVTUTKL+julkaisuja+11+Game+Player.pdf/9ff35e9b-3513-c490-c188-3e3f18e71bdd/PVTUTKL+julkaisuja+11+Game+Player.pdf.

44 Justin Sherman, 'Russia's Domestic Internet Is a Threat to the Global Internet', *Slate*, 24 October 2019, https://slate.com/technology/2019/10/russia-runet-disconnection-domestic-internet.html.

45 Union of Concerned Scientists, 'UCS Satellite Database', 1 January 2021, https://www.ucsusa.org/resources/satellite-database.

46 The data-localisation law was passed in 2015 and augmented in 2019 with tougher penalties for non-compliance. See Gorodissky and Partners, 'Russia Sets $280,000 Fine for Breaching Data Localization Law', 10 September 2019, https://www.lexology.com/library/detail.aspx?g=5b43dda3-d68f-4f5b-8767-9846b649b5d9.

47 'Russian court fines Twitter and Facebook 62,840 dollars each for refusing to localize user data', Meduza, 13 February 2020, https://meduza.io/en/news/2020/02/13/russian-court-fines-twitter-62-840-dollars-for-refusing-to-localize-user-data.

48 *Ibid*.

49 CERT-GIB was originally a Russian private-sector initiative, in 2011, which has since grown into a global business. See Group-IB, https://www.group-ib.com.

50 Gosudarstvennaya sistema obnaruzheniya, preduprezhdeniya i likvidatsii posledstvii komp'yuternikh atak

51 Dmitriy Kuznetsov, 'GosSOPKA: chto takoe, zachem nuzhna i kak ustroena', Anti-Malware.ru, 2 April 2019, https://www.anti-malware.ru/analytics/Technology_Analysis/gossopka-what-is-it-how-it-works. A list of the relevant laws and regulations, in Russian, can be found at 'Normativnye dokumenty v oblasti GosSOPKA i bezopasnosti KII', Positive Technologies, 23 July 2019, https://www.ptsecurity.com/ru-ru/research/knowledge-base/terminology-gossopka-kii-full-version.

52 Kuznetsov, 'GosSOPKA: chto takoe, zachem nuzhna i kak ustroena'.

53 '"InfoTeKS" podklyuchil pervyi region k GosSOPKA', Comnews, 12 July 2019, http://www.comnews.ru/content/120767/2019-07-12/infoteks-podklyuchil-pervyy-region-k-gossopka.

54 'Ob utverzhdenii Pravil predostavleniia subsidiy iz federal'nogo byudzheta na sozdanie otraslevogo tsentra Gosudarstvennoi sistemy obnaruzheniia, preduprezhdeniia likvidatsii posledstvii komp'iuternykh atak (GosSOPKA) i vklyuchenie ego v sistemu avtomatizirovannogo obmena informatsiei ob aktual'nykh kiberugrozakh', Ofitsial'nyi internet-portal pravovoi informatsii, 9 October 2019, http://publication.pravo.gov.ru/Document/View/0001201910090023.

55 '2020: Zapusk Tsentra monitoringa i reagirovaniia s pravom ispolniat' funktsii tsentra GosSOPKA', TAdviser, 5 March 2020, https://www.tadviser.ru/index.php/Продукт:Код_Безопасности:_Центр_ мониторинга_и_реагирования.

56 Valeria Pozychanyuk and Petr Mironenko, 'FSB potrebovala ot internet-servisov onlain-dostup k dannym i perepiske pol'zovatelei', The Bell, 11 February 2020, https://thebell.io/fsb-potrebovala-ot-internet-servisov-onlajn-dostup-k-dannym-i-perepiske-polzovatelej.

57 GMA Consult Group, 'Russia Authorizes 16 Preinstalled Applications for All Smartphones and Tablets', 20 December 2020, https://www.gma.trade/single-post/russia-authorizes-16-preinstalled-applications-for-all-smartphones-and-tablets.

58 'Russia: Growing Internet Isolation, Control, Censorship', Human Rights Watch, 18 June 2020, https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.

59 Kukkola, 'The Russian Segment of the Internet as a Resilient Battlefield', p. 117.

60 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

61 'DDoS attacks on Russian online retailers double in 2020', TASS, 16 February 2021, https://tass.com/economy/1256821.

62 'Data leaks from Banks of Russia', TAdviser, 29 January 2021, https://tadviser.com/index.php/Article:Date_leaks_from_Banks_of_Russia#.2A_The_number_of_leaks_from_the_financial_sector_in_Russia_grew_by_a_third.

63 Lawrence Abrams, 'Russian government warns of US retaliatory cyberattacks', Bleeping Computer, 23 January 2021, https://www.bleepingcomputer.com/news/security/russian-government-warns-of-us-retaliatory-cyberattacks/.

64 Presidential Administration, 'Federal Security Service Board meeting', 24 February 2021, http://en.kremlin.ru/events/president/news/65068.

65 Presidential Administration, 'Extended meeting of Russian Interior Ministry Board', 3 March 2021, http://en.kremlin.ru/events/president/news/65090.

66 Angelina Krechetova and Ekaterina Kinyakina, 'Minkomsviazi povelo itogi pervykh uchenii po zakonu o "suverennom RuNete"', *Vedomosti*, 23 December 2019, https://www.vedomosti.ru/technology/news/2019/12/23/819484-suverennom-runete.

67 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.

68 Alex Grigsby, 'Unpacking the Competing Russian and U.S. Cyberspace Resolutions at the United Nations', Council on Foreign Relations, 29 October 2018, https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations.

69 Anton Troianovski and David E. Sanger, 'Putin Wants a Truce in Cyberspace – While Denying Russian Interference', *New York Times*, 25 September 2020, https://www.nytimes.com/2020/09/25/world/europe/russia-cyber-security-meddling.html.

70 The OEWG's full name is the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. For details on its activities, see United Nations Office for Disarmament Affairs, 'Open-ended Working Group', https://www.un.org/disarmament/open-ended-working-group.

71 Michael Birnbaum, 'Russian submarines are prowling around vital undersea cables. It's making NATO nervous', *Washington Post*, 22 December 2017, https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html.

72 Andy Greenberg, 'A Brief History of Russian Hackers' Evolving False Flags', *Wired*, 21 October 2019, https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear.

73 Anton Troianovski and Ellen Nakashima, 'How Russia's military intelligence agency became the covert muscle in Putin's duels with the West', *Washington Post*, 28 December 2018, https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

74 'SBU Blocks 103 Russian Cyber Attacks to Prevent Theft of State Bodies Data: Security Service of Ukraine', Security Service of Ukraine, 6 May 2020, https://www.sbu.gov.ua/en/news/1/category/1/view/7559#.SMNp6d9O.dpbs.

75 White House, 'Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, February 17, 2021', https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021.

10. Iran

Iran regards itself as being in an intelligence and cyber war with its enemies. In 2010, when the Stuxnet attack on Iran by the United States and Israel was revealed, the country had little access to international cyber-security suppliers and only a very small number of domestic researchers in the field. Since then, however, it has become a determined cyber actor against US, Gulf Arab and Israeli interests. At the same time, a perceived need to quell domestic opposition through increased internal cyber surveillance has dovetailed with the government's desire to counter external threats. However, economic depression, political turmoil and internal deficiencies suggest that Iran will not be able to boost its indigenous cyber-defence capability easily or quickly. Its overall cyber capabilities do not match the scale and sophistication of its ballistic-missile or nuclear programme. For example, it lacks the resources, talent and technical infrastructure needed to develop and deploy sophisticated offensive cyber capabilities, even though it has used lower-level offensive cyber techniques widely, with some success. Iran is a third-tier cyber power that makes use of less sophisticated cyber technologies and operational capabilities to serve its strategic goals, which include espionage, power projection and strategic signalling.

Strategy and doctrine

Iran's approach to cyberspace is inherently bound to its domestic authoritarian policies and its international confrontations. The stage for current domestic policy was set in 2009 when the Islamic Revolutionary Guard Corps (IRGC) took over the Telecommunications Company of Iran after large-scale protests against the regime that were fuelled by social media.[1] The development of Iran's international cyber policy can be traced back to the Stuxnet attacks on the country that were revealed in 2010 and attributed to the United States and Israel.

In most areas related to security in cyberspace, Iran has not published any formal strategy documents or doctrines. The main indicators are therefore organisational reforms and associated legislation. The Iranian Cyber Army, a group of pro-regime hackers with presumed links to the IRGC and pledging loyalty to Supreme Leader Ayatollah Ali Khamenei, began operating in 2009 as the direct result of concern among conservative forces in Iran about anti-government and pro-Western internet-based propaganda. The armed forces set up a Cyber Defense Command in 2010, and in 2011 a Cyber Police Force was created with the aim of protecting 'national and religious identity, community values, legal liberty and critical national infrastructure from electronic attack'.[2]

List of acronyms

CERT	Computer Emergency Response Team
ICT	information and communications technology
IRGC	Islamic Revolutionary Guard Corps
IRGC-IO	Islamic Revolutionary Guard Corps Intelligence Organization
MOIS	Ministry of Intelligence and Security
NCC	National Cyberspace Center
NPDO	National Passive Defense Organization

A Supreme Council for Cyberspace, headed by the Supreme Leader, was created in 2012 with the twin goals of 'fully exploiting the positive potential of Iranian cyberspace' and 'protecting the country and people from the negative potential of cyberspace'.[3] Two of its more specific objectives were to provide government support to pro-regime hacker groups and to develop science, research, cultural policy and strategic studies related to cyberspace.[4]

In 2013, parliament passed a law to set up a National Cyberspace Center (NCC) with wide-ranging policy aims. The text of the legislation stated the aims of the NCC in such detail that it resembled the cyber-security strategy documents of some countries.[5] The provisions included expanding the country's sovereign ICT capability in the face of powerful global corporations. They foreshadowed an increase in domestic content for the World Wide Web, the promotion of religious and state ideology, and preparations for a 'culture war' with the country's enemies. The law also called for diplomatic actions on the international stage, aimed at limiting the influence of any superpower over governance of the internet and protecting what it called the 'international rights' of Iranian internet users. The NCC appears to have coordinating responsibilities on behalf of the Supreme Council across all the cyber organisations. In some areas of policy the Supreme Council has chosen to work directly with lower-level entities such as the Ministry of Information and Communications Technology.

On the international front, Iran remains preoccupied with the US, Israel and the Gulf Arab states. After carrying out successful cyber attacks against US banks in 2012 without significant retaliation, the Iranian regime felt that it was getting its cyberspace-security policy in order. An IRGC general declared in 2013 that Iran was the 'fourth-biggest cyber power among the world's cyber armies',[6] a claim based on unverified reports that the government could rely on a cyber militia force of 120,000 specialists. These appear to be exaggerated.

In 2019, the commander-in-chief of the IRGC, Major-General Hossein Salami, declared that Iran was 'in an atmosphere of full-blown intelligence war with the US' and other 'enemies of the Revolution and the Islamic system', with the country subjected to a combination of 'psychological warfare and cyber operations, military provocations, public diplomacy and intimidation tactics'.[7] In July 2020 the General Staff of the armed forces issued a declaration on Iran's view of its right to retaliate against cyber attacks, a document that could almost be regarded as an official statement of the country's cyber strategy.[8] Its aim was to clarify the 'concepts, macro policies and the framework of the activities of the armed forces against increasing and various threats of cyberspace'. The declaration stated that Iran would regard 'any intentional use of cyber force with tangible or non-tangible implications' within its borders as a violation of its sovereignty, and reserved the right to retaliate with military force if a cyber operation crossed the threshold of a 'conventionally armed attack'.

In summary, Iran's strategic outlook has a great bearing on its approach to the threats and opportunities that cyberspace presents. This is particularly the case with its doctrine of strategic depth, which is aimed against its traditional regional adversaries (Israel, and the Sunnis led by Saudi Arabia) and in which it perceives an opportunity to penetrate the networks of the US. Its cyber capabilities are also moulded by internal organisational rivalries. As with Iranian strategy in general, the approach to cyberspace has an innate duality, with pragmatic regional-security considerations coexisting uncomfortably with a more dogmatic attempt to protect and export Iran's Islamic Revolution.[9]

Governance, command and control

The Supreme Council for Cyberspace, chaired by the president, is Iran's highest policymaking authority in the field. It comprises 27 members from different areas of government and society, including the armed forces, the IRGC, the judiciary, parliament, state-run radio and television stations, the police, and the ministries of Information and Communications Technology, Intelligence and Security, Culture and Science. It oversees the regime's censorship policies as they apply to the internet, and regulates the country's internet exchange points (IXPs), network separation and content-filtering.[10]

The main cyber agencies in Iran are as follows:

- the NCC
- the National Passive Defense Organization (NPDO), responsible for cyber civil defence and the protection of critical infrastructure

- the Cyber Police
- the IRGC Intelligence Organization (IRGC-IO), responsible for offensive cyber operations
- Cyber Defense Command, part of the armed forces, and also involved in offensive cyber operations
- the Ministry of Intelligence and Security (MOIS), responsible for signals intelligence
- the Intelligence Protection Organizations within the armed forces and other government agencies.[11]

There are therefore five main channels of command: through the NCC, the IRGC, the armed forces, the MOIS and the civil sector (including the NPDO and the police, which often vie for influence). Through its militia force the Basij, the IRGC commands cyber units and proxies including the IRGC Electronic Warfare and Cyber Defense Organization and the Basij Cyber Council.[12]

The governance of cyber policy in Iran has developed through two decades of political turmoil, a sense of victimhood in the face of international confrontation and sanctions, and the imperative of defeating domestic and foreign enemies of the regime. The country has been involved in proxy wars in Iraq, Syria and Yemen, and there has been regular military tension with US and Israeli forces in the region. The Supreme Council for Cyberspace nominally provides a multi-stakeholder forum where non-political and non-military needs, such as cyber security for commercial enterprises, can be addressed. Although it does indeed carry out that role, national security is always a priority and has intensified since the assassinations in 2020 of Major-General Qasem Soleimani, the commander of the Quds Force in the IRGC,[13] and Mohsen Fakhrizadeh, who had led Iran's nuclear programme for more than two decades.[14]

Iran's national Computer Emergency Response Team (CERT) is under the direction of the Ministry of Information and Communications Technology. It cooperates with domestic agencies such as the Cyber Police and the NPDO's Cyber Defense Command, cybersecurity centres in Iranian universities and also foreign CERTs in order to protect Iran's cyberspace, investigate or mitigate incidents, and issue warnings.[15]

Core cyber-intelligence capability

The MOIS is Iran's primary signals-intelligence agency. Despite its designation as a ministry, and the fact that the minister is appointed by the president (subject to approval by the Supreme Leader), the MOIS acts more as an independent executive body. It has a remit to monitor domestic political threats, undertake foreign intelligence collection and conduct counter-intelligence operations.[16] It oversees all covert operations and usually carries out domestic operations itself, while the IRGC Quds Force runs extraterritorial operations such as sabotage, assassinations and human intelligence collection. It is the MOIS that cooperates with foreign intelligence agencies, most notably Russia's External Intelligence Service. The country's cyber-intelligence capabilities are probably affected by the duplication and competition that exist between its two main intelligence organisations, the IRGC-IO and the MOIS.[17] The IRGC-IO is perhaps the most powerful security agency in Iran and almost certainly plays a role in foreign and domestic cyber operations and in policy-setting.[18]

Iran continues to be outmatched by Israel in terms of regional intelligence reach, with Stuxnet just an early example. Though Iranian cyber operations have been detected in networks in the US, the United Kingdom and elsewhere, the speculative and unsophisticated nature of those operations suggests Iran lacks any meaningful global cyber-intelligence reach. It remains to be seen whether, in the wake of the Syrian conflict, Iranian capabilities might in time benefit from closer cooperation with Russia.

Little detail is known about the numbers of Iranian cyber-intelligence personnel or their level of training. However, the published budgets are small in comparison with those of states such as the UK. Skilled personnel with the right political allegiances are in short supply, and most Iranian cyber operations use basic techniques. Many of those operations are contracted out, especially to research institutes.[19]

Cyber empowerment and dependence

The Iranian government has declared high ambitions for the digital economy, though starting from a low base – in 2020 it stated that the digital sector accounted for 6.5% of GDP, in comparison with a global average of 15.5%.[20] In early 2020 the Supreme Council for Cyberspace

discussed a five-year plan[21] that would see the digital economy provide 10% of GDP by 2025 – potentially a significant expansion but still a far smaller contribution than those made by the ICT sectors of Iran's main adversaries, Israel and the US. Targets for 2024 include internet or mobile infrastructure to reach 80% of rural villages with more than 20 households, and 80% of Iranian households to have broadband access (with a speed of at least 20 Mbps).[22] In a global survey of digital inclusion covering the period 2017–20, Iran was one of the top ten most improved countries, though again starting from a low base – it was ranked only 37th overall.[23]

In 2020 the Ministry of Information and Communications Technology launched several infrastructure projects aimed at improving the country's digital economy. These include the construction of a data centre in Tehran, the development of the National Information Network – Iran's tightly controlled domestic internet, which has been under construction since 2013 – and a plan to support digital businesses impacted by the COVID-19 pandemic.[24] The data centre in Tehran, costing US$63 million, would purportedly increase Iran's overall data capacity by 25%. Another large-scale data centre has been built in Tabriz, contributing to the sustainability of Iran's network infrastructure and its capacity for cloud computing.[25]

Iran is among the top 20 countries in some areas of scientific research, including certain aspects of artificial intelligence (AI),[26] and Tehran appears in a list of the world's top 50 research clusters in terms of patentable research.[27] However, the level of investment in ICT research and development (R&D), both in the civilian and the military domains, is probably lower than in most countries with high ambitions in the sector: Iran spends less than 1% of GDP on government R&D across all sectors, a figure that rather contradicts the government narrative about its scientific ambitions.[28] Sanctions imposed on Iran have also created a difficult business environment for the country's tech start-ups and constrained their growth. Although they enjoyed a boom period from 2013 to 2016, many have since tried to relocate overseas.[29] In 2018, according to unofficial estimates, they accounted for less than 1% of GDP.[30]

The development of Iran's digital economy has been severely hampered by the authoritarian political environment and the consequences of geopolitical confrontation with Western countries, particularly sanctions related to Iran's lack of transparency over its international nuclear obligations. United Nations sanctions were in force from 2006 to 2015 and the US re-imposed its own sanctions in 2018 after withdrawing from the Joint Comprehensive Plan of Action (JCPOA). In 2016 and 2017, the first two years of the JCPOA, Iran's GDP grew by 12.5% and 3.7% respectively, but with the return of US sanctions it contracted by 5.4% in 2018 and 6.5% in 2019.[31] Even if the nuclear-related sanctions were to be lifted completely, opposition among Western states to other aspects of Iranian policy (on human rights, support for Hizbullah in Lebanon and relations with Israel) would continue to restrict ICT trade with European, North American, Japanese and South Korean firms.

Iran is among the top 20 countries in some areas of scientific research, including certain aspects of AI

Among the states actively involved in AI research, Iran is one of the least advanced. It was placed 33rd, for example, in a ranking based on contributions to the two most prestigious AI conferences in 2020.[32] For AI in health/medicine research it has been ranked higher, for example in lists of the top countries according to numbers of published articles (12th position) and citation rate (16th).[33] Iran is looking to augment its AI research capabilities through cooperation with Russia.[34] It has been applying AI in the military domain, for example in a large-scale drone-combat drill[35] and in the coordination of exercises involving air, sea and land assets.[36]

Iran's space programme has been developing slowly for two decades, with a mixture of civil-sector scientific inputs and very important military involvement (principally the ballistic-missile programme).[37] Its satellite-launch programme for civil-sector research began in 2009. After several failed launches of civilian satellites in 2019 and early 2020, the IRGC successfully launched its first military-reconnaissance satellite, *Noor*, in April

2020, using a previously unknown space-launch vehicle.[38] While *Noor* is expected to be used for intelligence-gathering and securing communications for the military, Iran's progress in satellite launches has aroused concerns about its possible use of the same technology in its missile programme.[39] In February 2021 the country successfully test-launched a new rocket capable of lifting a 220-kilogram satellite.[40]

Cyber security and resilience

Given the Iranian regime's premium on secrecy and deception, it is perhaps unsurprising that it has never published a meaningful cyber strategy. That does not mean, however, that no coherent strategy exists. Attempts have been made to improve the systems for handling cyber emergencies. The NPDO, a quasi-military entity staffed mostly by IRGC and Basij personnel, is tasked with protecting critical national infrastructure. Its role and budget have expanded steadily since its formation in 2003.[41]

The Ministry of Information and Communications Technology is responsible for the development of a National Information Network designed to improve the security of internal data centres and ensure necessary bandwidth. The regulation establishing the Supreme Council for Cyberspace called for increased national-level cyber training, as well as improvements to Iran's systems for detection, warning and information-sharing.[42] The NPDO began conducting modest cyber-defence exercises in 2010,[43] and other agencies have also reported occasional exercises since then. In 2018 the NCC set up a special task force to counter US cyber operations and the armed forces announced a new, secure communications system that they said was domestically designed and produced.[44] In 2019 the Ministry of Information and Communications Technology announced that it was implementing a cyber-defence programme called 'Digital Fortress'.[45] Overall, however, Iran's scientific capabilities in the area of cyber defence are not advanced, and there is little in the way of government planning that seems likely to change that.[46]

Iran ranked only 60th out of 175 countries in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union (ITU).[47] The ITU had previously highlighted the country's lack of officially approved national cyber-security frameworks, including for implementing recognised standards and accreditation across the public and private sectors.[48] Similarly, Iran still does not have any government-backed national benchmarking system for assessing cyber security. The global professional body for information-security professionals, ISACA, has chapters in 188 countries but none in Iran.[49]

Global leadership in cyberspace affairs

Iran's cyber diplomacy has mainly focused on highlighting attacks against it by the US and Israel, with much made of the Stuxnet attack in particular. Like China and Russia, it wishes to reshape the future of cyberspace and contest its domination by the West. However, unlike China (or India for that matter), it does not have sufficient technical resources to do so, either globally or within its region, and it also lacks the diplomatic firepower to coalesce with other states in a way that would significantly influence international cyberspace policy.

Nevertheless, Iran participates in several international cyber initiatives. For example, the Ministry of Information and Communications Technology declares periodic civil cyber exercises with Russian partners, listing several Iranian university cyber centres as participants.[50] Iran is an observer to the Shanghai Cooperation Organisation, which is one of the main vehicles used by Russia and China to promote their agenda on internet sovereignty, a vision that Tehran shares. The national CERT is part of the team operated by the Organisation of Islamic Cooperation (OIC-CERT) and is a member of the Cybersecurity Alliance for Mutual Progress led by South Korea's Internet and Security Agency.[51] Overall, though, Iran's priority has been its own cyber security rather than a broader role in global cyberspace affairs.

Offensive cyber capability

The Iranian regime first acknowledged its use of an offensive cyber capability in 2010, when it disrupted the website of a domestic human-rights group in response to dissidents' use of social media during the country's unrest in 2009. It is likely that domestic dissidents have remained a priority target ever since.

Iran's first use of disruptive cyber capabilities against foreign targets, following the discovery of the Stuxnet virus in its nuclear centrifuges in 2010, was a series of basic denial-of-service attacks against banks in the US in 2012.[52] Later in 2012 it carried out an attack against Saudi Aramco that was more audacious, using a wiper virus (Shamoon) that disabled 30,000 computers. Disruptive and destructive cyber operations have remained a staple of Iranian statecraft, though used quite sparingly.[53] Information operations on Western social-media platforms, a new Iranian tactic, emerged from around 2018.[54] In 2020 Iran was allegedly behind an unsuccessful cyber attack intended to disrupt Israeli critical national infrastructure (water supply and wastewater treatment).[55] It also allegedly carried out attacks against more than 80 Israeli companies in retaliation for the November 2020 assassination of Fakhrizadeh, which it attributed to Israel.[56] These included infiltrating the systems of Israel's largest defence contractor and leaking its data.[57]

While Iran has continued to conduct cyber operations further afield, for example into commercial networks in the US, most of these appear to have been speculative and mainly for the purpose of data theft rather than disruption. Its 2013 breach of the network of a small dam near New York appears to have been an interesting exception – it may have been an attempt to pre-position a cyber capability on US critical national infrastructure. But perhaps it also indicated the limits of Iran's cyber-intelligence reach, as the dam was tiny in comparison to some of the United States' colossal hydroelectric structures.[58]

Overall, Iran has deployed offensive cyber for diverse goals and against a range of targets worldwide. Its cumulative experience now represents a relatively high level of operational maturity, with the regime's embrace of cyber operations firmly established as a useful instrument of national power. Most strikingly, cyber capabilities have enabled Iran to reach and deliver effect into the US in ways it cannot achieve with conventional capabilities. Nevertheless, the operations lack technical sophistication. They show little sign of innovative indigenous techniques or procedures and seem to be readily detected and attributed by Western companies. In part this may be the result of relying on research institutes in universities to devise and execute many of the attacks. Iran's cyber capabilities are much less developed than those of the West, both in quality and scale. Within its region its capabilities are certainly outmatched by those of Israel, although Tehran has had successes in offensive cyber against Saudi Arabia[59] and some of the anti-government groups in Syria.[60]

Notes

1 Daniel Baldino and Jarrad Goold, 'Iran and the emergence of information and communications technology: The evolution of revolution?', *Australian Journal of International Affairs*, vol. 68, no. 1, 2014, pp. 17–35, p. 28.

2 See United Nations Institute for Disarmament Research, UNIDIR Cyber Policy Portal, 'Iran (Islamic Republic of)', https://cyberpolicyportal.org/en/state-pdf-export/eyJjb3VudHJ5X2dyb3VwX2lkIjoiNjUifQ.

3 See Small Media, 'Iranian Internet Infrastructure and Policy Report', February 2014, p. 3, https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf.

4 *Ibid.*, p. 7.

5 *Ibid.*, p. 4.

6 'Iran Enjoys 4th Biggest Cyber Army in World', Ahlul Bayt News Agency, 2 February 2013, https://en.abna24.com/service/iran/archive/2013/02/02/387239/story.html.

7 Zak Doffman, 'Iran: "We Will Beat U.S. in Intelligence War" and "Punish Mistakes With Crushing Strikes"', *Forbes*, 19 May 2019, https://www.forbes.com/sites/zakdoffman/2019/05/19/iran-we-will-beat-u-s-in-intelligence-war-and-punish-mistakes-with-crushing-strikes/?sh=9a225d25e16d.

8 'General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat', Fars News Agency, 17 August 2020, https://www.farsnews.ir/en/news/13990527000544/General-Saff-f-Iranian-Armed-Frces-Warns-f-Tgh-Reacin-Any-Cyber-Threa.

9 See also International Institute for Strategic Studies, *Iran's Networks of Influence in the Middle East* (London: IISS, 2019), pp. 27–8.

10 Official Gazette of Iran, 'Mosavabbe shoraye aali fazaye majazi dar khosoos siyasat haye hakem bar rah andazi noghat

tabadol terrafik dakheili (IXP) va ijad tamayoz beyne', 22 March 2013, http://www.rooznamehrasmi.ir/laws/ShowLaw.aspx?Code=1152.

11 The Intelligence Protection Organisations operate as counter-intelligence agencies, but also act as political police to suppress opponents of the regime.

12 Congressional Research Service, 'Iranian Offensive Cyber Attack Capabilities', 13 January 2020, https://fas.org/sgp/crs/mideast/IF11406.pdf.

13 'Qasem Soleimani: US strike on Iran general was unlawful, UN expert says', BBC News, 9 July 2020, https://www.bbc.com/news/world-middle-east-53345885. According to the BBC, Soleimani was one of the most powerful intelligence officials in Iran, with a role that included directing clandestine missions in other countries.

14 'Mohsen Fakhrizadeh: "Machine-gun with AI" used to kill Iran scientist', BBC News, 7 December 2020, https://www.bbc.com/news/world-middle-east-55214359.

15 See 'Markazeh modiriyat emdaad va hamahangie amaliyate rokhdad haye rayaneh ei', https://cert.ir/index.

16 Carl Anthony Wege, 'Iran's Intelligence Establishment', *Intelligencer*, Summer 2015, pp. 64–5, https://www.afio.com/publications/WEGE%20Iranian%20Intel%20Services%202015%20Sep%2001%20FINAL.pdf.

17 Eric Randolph, 'Iranian IRGC consolidates primacy in intelligence operations', Janes, 19 August 2020, https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-in-intelligence-operations.

18 Insikt Group, 'Despite Infighting and Volatility, Iran Maintains Aggressive Cyber Operations Structure', Recorded Future, 2020, pp. 13–21, https://go.recordedfuture.com/hubfs/reports/cta-2020-0409.pdf.

19 Levi Gundert, Sanil Chohan and Greg Lesnewich, 'Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations', Future', 2018, https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf.

20 'Iran Unveils Four Mega Projects to Boost Digital Economy', IFP News, 28 May 2020, https://ifpnews.com/iran-unveils-four-mega-projects-to-boost-digital-economy. For an assessment by Iranian economists, see Amir Hossein Mozayani and Niloofar Moradhassel, 'How Much Has ICT Contributed to Iran Economic Growth', *International Journal of Economics and Politics*, vol. 1, no. 1, 2020, pp. 57–68, http://jep.sbu.ac.ir/article_87384.html.

21 'Iran Gov't Outlines Projects to Expand Digital Economy', *Financial Tribune*, 2 February 2020, https://financialtribune.com/articles/sci-tech/101979/iran-gov-t-outlines-projects-to-expand-digital-economy.

22 Jamal Sophieh, 'An Overview of Digital Economy and Digital Transformation in Iran', Ministry of Information and Communications Technology, workshop presentation, July 2019, p. 22, https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2019/jul-iran-dtx/Workshop-on-%E2%80%9CDigital-Transformation-in-Digital-Economy%E2%80%9D/Session%2014%20-%20Iran.pdf.

23 'Qatar, UAE, Iran and Egypt Making Big Strides in Digital Inclusion', Consultancy-me.com, 3 March 2021, https://www.consultancy-me.com/news/3430/qatar-uae-iran-and-egypt-making-big-strides-in-digital-inclusion.

24 'Iran Unveils Four Mega Projects to Boost Digital Economy', Iran Front Page, 28 May 2020, https://ifpnews.com/iran-unveils-four-mega-projects-to-boost-digital-economy.

25 'Iran to Open Second Largest Data Center over Weekend: Minister', Pars Today, 25 June 2020, https://parstoday.com/en/news/iran-i122999.

26 See S.F. Wamba et al., 'Are we preparing for a good AI society? A bibliometric review and research agenda', *Technological Forecasting and Social Change*, 2020, https://www.sciencedirect.com/science/article/abs/pii/S0040162520313081?dgcid=rss_sd_all; and Jiqiang Niu et al., 'Global research on artificial intelligence from 1990–2014: Spatially-explicit bibliometric analysis', *ISPRS International Journal of Geo-Information*, vol. 5, no. 66, pp. 7–9, https://www.mdpi.com/2220-9964/5/5/66/pdf.

27 Kyle Bergquist and Carsten Fink, 'The Top 100 Science and Technology Clusters', World Intellectual Property Organisation, 2020, p. 44, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020-chapter2.pdf.

28 Mehdi Garshasbi, 'R&D still unappreciated', *Tehran Times*, 2 January 2021, https://www.tehrantimes.com/news/456487/R-D-still-unappreciated.

29 Mohsen Tavakol, 'Sanctions and Domestic Constraints Cripple Iran's Startups', Atlantic Council, 7 February 2020, https://www.atlanticcouncil.org/blogs/iransource/sanctions-and-domestic-constraints-cripple-irans-startups/.

30 Najmeh Bozorgmehr, 'Start-up Republic: Can Iran's Booming Tech Sector Thrive?', *Financial Times*, 17 April 2018, https://www.ft.com/content/ca7ab580-3d71-11e8-b9f9-de94fa33a81e.

31 International Monetary Fund, 'Islamic Republic of Iran', October 2020, https://www.imf.org/en/Countries/IRN.

32 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.

33 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.

34 'Iran, Russia to Cooperate on Artificial Intelligence Research', Islamic Republic News Agency, 3 September 2020, https://en.irna.ir/news/84025992/Iran-Russia-to-cooperate-on-artificial-intelligence-research.

35 'Iran uses "artificial Intelligence" in drone drill', Mehr News Agency, 7 January 2021, https://en.mehrnews.com/news/168208/Iran-uses-artificial-intelligence-in-drone-drill.

36 Michael Rubin, 'Even Iran Wants an AI-Powered Military Drones', *National Interest*, 25 December 2020, https://nationalinterest.org/blog/reboot/even-iran-wants-ai-powered-military-drones-175202.

37 Andrew Hanna, 'Iran's Ambitious Space Program', The Iran Primer, United States Institute for Peace, updated 1 February 2021, https://iranprimer.usip.org/blog/2020/jun/23/iran%E2%80%99s-ambitious-space-program.

38 'Iran Launches Its First Military Satellite', Al-Jazeera, 22 April 2020, https://www.aljazeera.com/news/2020/4/22/iran-launches-its-first-military-satellite.

39 Michael Elleman and Mahsa Rouhi, 'The IRGC Gets into the Space-Launch Business', International Institute for Strategic Studies blog, 1 May 2020, https://www.iiss.org/blogs/analysis/2020/05/iran-military-satellite-launch-irgc.

40 Hanna, 'Iran's Ambitious Space Program'.

41 Farzin Nadimi, 'Iran's Passive Defense Organisation: Another Target for Sanctions', The Washington Institute, 16 August 2018, https://www.washingtoninstitute.org/policy-analysis/view/irans-passive-defense-organization-another-target-for-sanctions.

42 Mehdi Safari, Hesam Seyedin and Katayoun Jahangiri, 'Disaster risk governance in Iran: Document analysis', *Journal of Education and Health Promotion*, vol. 8, 2019, Table 5, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6691616.

43 BBC Monitoring, 'Iranian Passive Defence Organization organizes "cyber exercises"', Islamic Republic News Agency, 21 August 2011. The head of the NPDO, Brigadier-General Gholamreza Jalali, reported in October 2019 that it had held five exercises in the year from 21 March 2018 to 20 March 2019, focusing on the 'functioning of cyberspace and the internet'. Among the conclusions drawn was that '85% of the country's infrastructures can keep operating if the Internet is cut off'. He also reported plans to conduct 64 exercises during the following two months. See 'Tehran: No Sign of US Cyber Attack after Drone Downing', Fars News Agency, 21 October 2019, https://www.farsnews.ir/en/news/13980729000775/Tehran-N-Sign-f-US-Cyber-Aack-afer-Drne-Dwning.

44 'Defense Minister unveils Iran's new cyber achievements', Iran Press, 22 December 2018, https://iranpress.com/en/iran-i130976-defense_minister_unveils_iran's_new_cyber_achievements.

45 Khosro Kalbasi, 'Iran Sets Up Digital Fortress to Forestall Rising Cyber Threats', *Financial Tribune*, 19 May 2019, https://financialtribune.com/articles/sci-tech/98058/iran-sets-up-digital-fortress-to-forestall-rising-cyber-threats.

46 See Y.M. Ramezan et al., 'The Role and Influence of the Digital Economy on the Strategic Model for Development of Cryptographic Science and Technology in the Islamic Republic of Iran', *Journal of National Security*, vol. 10, no. 35, Spring 2020, pp. 327–58, https://www.sid.ir/en/journal/ViewPaper.aspx?ID=749286. The *Journal of National Security* is published by the Supreme National Defense University of Iran. In the abstract of their article, the authors state that 'the main issue … is the lack of a well-designed and strategic model for the development of cryptographic science and technology'.

47 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 64, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

48 International Telecommunication Union, 'Global Cybersecurity Index & Cyberwellness Profiles', 2015, p. 242, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

49 ISACA – formerly the Information Systems Audit and Control Association, but now known only by its acronym – is dedicated to system security. See http://www.isaca.org.

50 For more information on the partner centres, see https://cert.ir/partners.

51 The Cybersecurity Alliance for Mutual Progress brings together government bodies, public organisations and non-profit organisations from 46 countries (as of 2020), most of which are developing economies. See https://www.cybersec-alliance.org/camp/membership.do.

52 For some background, see 'U.S.–Iran Tensions: Implications for Homeland Security', Hearing before the Committee on Homeland Security, House of Representatives, 116th Congress, 2nd Session, 15 January 2020, https://www.

govinfo.gov/content/pkg/CHRG-116hhrg41269/html/CHRG-116hhrg41269.htm.

53 For a list of similar attacks in the years since 2012, see Andrew Hanna, 'The Invisible U.S.–Iran Cyber War', The Iran Primer, United States Institute for Peace, updated 5 November 2020, https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war.

54 Ed Parsons and George Michael, 'Understanding the Cyber Threat from Iran', F-Secure, undated, https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran.

55 Catalin Cimpanu, 'Two more cyber-attacks hit Israel's water system', ZDNet, 20 July 2020, https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/.

56 Jacob J, 'Iranian Hacker Group Pay2Key Attacks Top Israeli Defense Corporation, Leaks Data on Dark Web', *International Business Times*, 21 December 2020, https://www.ibtimes.sg/iranian-hacker-group-pay2key-attacks-top-israeli-defense-corporation-leaks-data-dark-web-54341.

57 Omer Benjakob, 'Iranian Cyberattack Claims New Victim – and Israeli Hackers Vow Revenge', *Haaretz*, 4 January 2021, https://www.haaretz.com/israel-news/tech-news/.premium.HIGHLIGHT-iranian-cyberattack-claims-new-victim-and-israeli-hackers-vow-revenge-1.9404606.

58 'Seven Iranian Hackers Indicted over Alleged Cyber Attacks Targeting US Banks and NY Dam', Trend Micro, 29 March 2016, https://www.trendmicro.com/vinfo/de/security/news/cyber-attacks/seven-iranian-hackers-indicted-over-attacks-on-banks-ny-dam.

59 Seth G. Jones et al., 'Iran's Threat to Saudi Critical Infrastructure: The Implications of U.S.–Iranian Escalation', CSIS, August 2019, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Jones_IransThreatSaudi_layout_UPDATE_09.17.pdf.

60 Insikt Group, 'Despite Infighting and Volatility, Iran Maintains Aggressive Cyber Operations Structure', Recorded Future, 2020, p. 16, https://go.recordedfuture.com/hubfs/reports/cta-2020-0409.pdf.

11. North Korea

North Korea's cyber strategy is probably not formalised and its operations have been characterised by opportunism. Little is known of its cyber-policy ecosystem. Since 2015 its publicly revealed cyber activity has consisted mainly of large-scale cyber fraud and extortion as a way of bolstering the country's access to hard currency. It has also carried out acts of cyber sabotage, including in retaliation for perceived insults to the leadership of the ruling Korean Workers' Party. Control of cyber policy is firmly in the hands of the leadership, operating through the structures of the party and the armed forces. North Korea lacks any sophisticated cyber-intelligence capability. It has a basic digital ecosystem, with between three and five million devices connected to internal mobile networks, including via a government intranet. Access to the global internet is strictly controlled by the government and depends on a very small number of gateways provided by Chinese and Russian service providers – a lack of diversity that makes the connections highly vulnerable to disruption. The country's level of cyber security is among the lowest in the world. North Korea's undertakings in cyberspace are hampered by a low cyber-skills base, largely the result of its self-imposed isolation, weak education system and underdeveloped ICT sector. It has played almost no part in global cyber diplomacy and has few international relationships to support its cyber ambitions. Despite its penchant for conducting offensive cyber operations, the techniques used are relatively basic, as it lacks the capability for sustained or sophisticated operations. Overall, though its cyber operations have achieved some global notoriety, North Korea is a third-tier cyber power.

Strategy and doctrine

There is little evidence that North Korea has a formal cyber strategy or doctrine. Its approach can be gleaned partly from statements by the leadership, but conclusions must otherwise be based on its observed activity. The statements suggest North Korea has a mixture of grandiose and more conventional ideas about the use of cyber operations during military conflict. The observed activity suggests the country's priorities are domestic surveillance, threatening South Korea, stealing money to gain access to hard currency otherwise unavailable because of financial and trade sanctions, classic espionage (especially relating to strategic weapons systems), and the occasional high-profile use of cyber operations to score retaliatory geopolitical points.

According to South Korean sources, North Korean leader Kim Jong-un views cyber power as central to modern political and military competition.[1] He is also reported to have said prior to 2013 that 'cyber warfare is an all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capability,

List of acronyms

ICT information and communications technology
KWP Korean Workers' Party
RGB Reconnaissance General Bureau

along with nuclear weapons and missiles'.[2] His father and predecessor as leader, Kim Jong-il, is reported to have expressed similar sentiments. In 2010 he is reported to have said: 'If warfare was about bullets and oil until now, warfare in the twenty-first century is about information. War is won and lost by who has greater access to the adversary's military technical information in peacetime, how effectively one can disrupt the adversary's military command-and-control information, and how effectively one can utilise one's own information.'[3]

Beyond this, North Korea's strategy and doctrine have to be deduced from what is known of the country's history of cyber attacks. Some analysts have attributed a reasonable degree of coherence to its cyber operations. The United States Department of Defense, for example, has suggested that North Korea is able to leverage the asymmetric edge that the cyber domain provides as part of a 'coercive diplomacy strategy'.[4]

However, few North Korean attacks have reached the threshold that might be associated with the idea of coercion.[5] Most attacks have resembled outlaw raids, including acts of retaliation, rather than a facet of sustained diplomacy. The main exception to this, and one that receives too little attention in the media, is the consistent cyber pressure North Korea exerts on South Korea's institutions and civil infrastructure, including public threats in 2014 against its civil nuclear industry.[6] One of the most prominent examples of retaliation by sabotage was the compromising of Sony Pictures' servers in 2014 before the release of *The Interview*, a comedy deriding Kim Jong-un. Internal emails and employees' personal data were leaked, and company computers wiped clean.[7]

In the wake of the economic sanctions imposed by the United Nations in 2013, North Korea sought new ways to finance its cyber activities. From 2014 onwards, experts detected, and attributed to North Korea, a series of complex extortion schemes and attacks on financial institutions and cryptocurrency dealers. A UN report in 2019 estimated that the gains from such operations totalled US$2 billion.[8] One of the operations, in 2017, used the WannaCry ransomware in an unsophisticated and uncontrolled way: the attack caused much more widespread damage than it intended, shutting down untargeted computers in public services, institutions, corporations and homes in about 150 countries.[9]

North Korea has also engaged in industrial espionage, with the armed forces targeting industries in the aerospace, high-tech and manufacturing sectors in South Korea and elsewhere in Asia. In 2020 the UN Security Council Sanctions Committee on North Korea published a detailed report on the country's criminal activities in cyberspace, which consisted of stealing money from banks to fund the nuclear-weapons and missile-development programmes that are subject to UN sanctions.[10]

The North Korean armed forces are believed to have developed offensive cyber capabilities for military purposes, with the aim of aiding conventional operations as part of its 'quick war, quick end' strategy.[11] Also known as the 'short and decisive strategy', this adopts a blitzkrieg-like model of fast manoeuvre and local overwhelming force.[12] But there is scant public evidence of planning or capability for sustained military cyber operations beyond classic electronic warfare. In wartime, North Korea would be likely to use cyber weapons against South Korean civilian infrastructure and could probably cause severe disruption even with limited attacks. The country is likely also to have developed plans to target South Korean military command-and-control assets or other military systems.

Governance, command and control

North Korea's cyber operations are conducted by the armed forces and the intelligence agencies under the direction of the Korean Workers' Party (KWP). Kim Jong-un, as leader of the KWP and chairman of the National Defense Commission, can exert direct control over such operations. This direct connection between the leadership and the cyber units potentially increases the price of failure for the personnel involved.

The Reconnaissance General Bureau (RGB, also known as Unit 586) is the main intelligence organisation. It was created in 2009 within the structure of the General Staff of the armed forces, but most sources assume it now operates independently of the General Staff and reports directly to the leadership.

As for which units of the RGB are involved in cyber operations, there are contradictory reports around the structures and names. The lead cyber agency appears to be the Cyber Warfare Guidance Unit (also referred to as

Unit 121 or Bureau 121).[13] Its missions include assessment of enemy computer systems and network vulnerabilities, exploiting such vulnerabilities for disruptive effect, and committing financial cyber crimes. Unit 121 appears to be subordinate to the Technical Bureau of the RGB. At least one source suggests it was set up in 2013 or 2014, and the 2014 Sony Pictures hack was attributed to it.[14]

There are reports suggesting that other units are becoming more prominent, most notably Lab 110 (though this may just be a reorganised version of Unit 121 or a sub-unit of it). Identified units that are part of Lab 110, or related to it, include:

- Office 98, which focuses on surveillance of defectors (and their support networks) and university professors in South Korea and overseas
- Office 414, with facilities in China as well as Pyongyang, which targets foreign governments and corporations for espionage and possible disruption
- Office 35, the technical bureau, which develops malware and explores adversaries' cyber vulnerabilities.[15]

Unit 91, probably at the same administrative level as Lab 110, is responsible for high-priority projects such as targeting South Korea's civil infrastructure and for cyber espionage against foreign targets possessing nuclear and weapons-related technology.[16] Unit 180 undertakes criminal cyber activities against foreign targets for the purpose of stealing money.[17]

Cyber-security companies in the West often refer to the RGB as 'APT38' (the acronym stands for 'advanced persistent threat'), and another distinct group, 'APT37', has also been identified.[18] The latter is known for covering its tracks by aggressively destroying forensic evidence.[19] 'Lazarus' and 'TEMP. Hermit' are the names given to two other groups connected to the RGB. Although they all differ in their targeting patterns, some appear to be sharing tools and personnel.[20] The nature of their relationships with the RGB, including the degree to which they are controlled by it, remains unknown.

The General Staff reportedly also controls other cyber units apart from the RGB. According to the cyber-security company FireEye, these units focus on intimidation, industrial espionage and preparations for high-intensity conflict, in which their role would be to disrupt adversaries' command-and-control systems in support of conventional military operations. Their targets are not only other countries' armed forces and industries but also a diverse group of foreign anti-regime activists, researchers and journalists.[21]

Core cyber-intelligence capability

While little is known about North Korean core cyber-intelligence capabilities, it is safe to assume they have two main priorities: regime continuity and early warning against military attack by the South Korean and US military forces stationed on or near the Korean Peninsula. Intelligence operations are also used to steal money from the international financial system to help mitigate the effects of economic sanctions.

The restrictions on internet access inside North Korea make it relatively easy for the regime to conduct comprehensive surveillance of internet use. This would allow most of North Korea's cyber-intelligence effort to be directed at the South Korean and US military forces. Beyond the Korean Peninsula, however, it is likely that North Korea's cyber-intelligence reach is very limited, except for small-scale, short-term operations. The operations that have been detected suggest a low level of tradecraft, though according to US assessments it is becoming more sophisticated.[22]

According to reports from defectors, the total number of personnel in North Korea's cyber units increased to about 3,000 under Kim Jong-il and then to 6,000 under Kim Jong-un , with most of the increase absorbed by Unit 121 of the RGB.[23] A 2021 report suggests there has been a small further increase, to 6,800 personnel, but that only 1,700 of them are 'hackers'.[24] The more specialised personnel are unlikely to be highly skilled, given the low throughput of IT graduates from the North Korean education system and their limited access to leading ICT technologies. The majority of the hackers are probably involved in espionage. The number of North Korean citizens formally educated in cyber technologies and eligible for recruitment into the cyber-intelligence units is estimated to be quite low, with only around 100 students per year graduating from the relevant courses at the principal military university.[25]

Cyber empowerment and dependence

North Korea aims for total national self-reliance, including in advanced technology. However, the country's economy and education system provide very weak foundations for this aspiration.[26] Its people and businesses are denied access to the knowledge and wealth-creation opportunities available via the World Wide Web.

The main mobile-phone network in North Korea was introduced in 2008, when the 3G mobile network Koryolink was first established through a joint venture by Orascom Telecom Holding, an Egyptian company, and the Korea Post and Telecommunications Corporation.[27] The Chinese company Huawei was the underlying supplier that laid the foundations for Koryolink's telecommunications structure, including network integration and software services; it also helped build a local encryption system.[28] In 2014 an estimated 2.8 million North Koreans, out of a population of about 25m, were using the Koryolink network.[29] By 2019 the total number of mobile-phone users had risen to about 5m.[30] North Korea's mobile networks do not have direct access to the global internet and must instead operate via the government's intranet.[31] The only mobile-phone users permitted to access the internet are within the higher echelons of the KWP – fewer than 10,000 people in total – and that access is encrypted.

In the .kp range there are reportedly only nine top-level domains (such as co.kp, gov.kp and edu.kp) and around 25 subdomains available.[32] Apart from using the IP addresses provided through these domains, North Koreans with permission to do so can access the internet through one Chinese and one Russian outlet, respectively China Netcom and a Russian satellite company apparently based in Lebanon.[33] It seems the country's ruling elite are internet savvy and also conscious of cyber security.[34] It has been reported that their use of the internet surged by 300% between 2017 and 2019, and that much of the increase was due to the cyber-crime operations aimed at alleviating the financial impact of UN and US sanctions.[35]

In addition to restrictions on internet access, the regime imposes controls in other parts of the network. For example, in order to facilitate government surveillance, the use of North Korea's local Wi-Fi service (Mirae) requires a SIM card for access. North Korea has also developed a modified Linux operating system, Red Star, that can track users' movements.[36] Red Star was developed by the regime's IT-research institute, the Korean Computer Center, which was made into a commercial enterprise in 2015.[37] Ownership of a computer depends on government approval, but many users can access US software.[38]

North Korea possesses notable software-development capabilities[39] and has sought to emulate India by becoming a hub for production outsourced by neighbouring countries (China, Japan and South Korea).[40] Its tech firms, often operating behind front companies, offer a wide range of capabilities to international customers, including website and app development,[41] business-management software, biometric-identification applications, virtual private networks and facial-recognition software.[42]

North Korea's people and businesses are denied access to the knowledge and wealth-creation opportunities available via the World Wide Web

The country has an active, if modest, space programme and has successfully launched two satellites,[43] in 2012 and 2016, following three failed attempts.[44] Although these satellites could potentially be used for reconnaissance and precision-targeting purposes for its missile programmes,[45] there is little publicly available evidence of North Korea attempting to establish a civil-sector space-industrial base.[46]

North Korea's education system focuses on nurturing technological talent, especially in its top universities – Kim Il-sung University, Kim Chaek University of Technology and Pyongyang University of Science and Technology. Courses in hacking are offered at Moranbong University, with outstanding programmers handpicked to attend.[47] The existence of the new Kim Jong-un University of National Defense, which is likely to focus on science and technology, was revealed

in 2020.[48] For younger students, computing courses are part of the curriculum from elementary school onwards.

Cyber security and resilience

North Korea has very weak cyber defences, as indicated by its very low position –171st out of 175 countries – in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union (ITU).[49] This stems from a low average level of technical skills and the government's policy of isolation from the outside world – in comparison, even China has made use of foreign specialists, including from the US, to help develop national cyber security. There is no publicly available plan for national cyber defence.

Although North Korea does not depend on the global internet to the same degree as other states, it cannot entirely isolate itself. The fact that it relies on only two international internet gateways is a key vulnerability, and often even means that its hacker teams can only be effective if deployed outside the country. Attacks aimed at disrupting North Korea's internet connectivity have been a regular occurrence.[50] An attack in March 2013 that severely restricted internet access[51] seems to have been retaliation by the US and South Korea after North Korean denial-of-service attacks against South Korean television networks and banks. In 2014 there was an internet blackout for two days after US president Barack Obama threatened retaliation for the attack on Sony Pictures.[52] In 2018 the US announced a policy of 'defend forward' in cyberspace, aimed at disrupting the malicious behaviour in cyberspace of countries including North Korea.[53] In a conflict it would potentially be easy for an adversary to deny North Korea all internet access by closing down the two gateways it operates.

Though digital systems are not part of the daily lives of the majority of North Koreans, they are crucial for the country's power stations and other infrastructure, including communications. Most of the power stations have antiquated electronic control systems and are likely to be highly insecure. The most modern include the four hydroelectric plants jointly operated by China, but these too would still be highly vulnerable to cyber attack. Since the majority of North Koreans already live without electricity in their homes, Western states would have few qualms about targeting cyber attacks at the national grid during a conflict.

Global leadership in cyberspace affairs

As a member of the UN, North Korea has a place in organisations such as the ITU and at forums such as the World Summit on the Information Society, but it has no record of diplomatic action on cyber norms and policies, or technical standards, that could be regarded as leadership. Its diplomatic interventions on such subjects are rare. In the UN General Assembly it regularly votes with Russia and China on annual resolutions on cyberspace issues – in 2018, for example, it voted with 118 other countries (against 46 Western-aligned ones) to support a resolution backed by Russia and China to establish the UN Open-Ended Working Group on international-security aspects of ICT developments.

Offensive cyber capability

North Korea has regularly conducted offensive cyber operations against South Korea since at least 2009. These have usually consisted of basic denial-of-service attacks against, and leaking or wiping of data from, internet-facing government and private-sector sites. Since the imposition of harsher UN sanctions in 2013, North Korea has used cyber capabilities to steal money from the global financial system: targets have included the SWIFT international-banking system, and banks in Bangladesh, Chile, South Korea, Taiwan and Vietnam. It also famously hacked and leaked data from Sony Pictures in 2014 and was responsible for the indiscriminate 2017 WannaCry attack. A 2020 report by the US Cybersecurity and Infrastructure Security Agency highlighted the ongoing threat that North Korean cyber operations pose to the stability of the international financial system.[54] There are also indications of some basic North Korean cyber-reconnaissance activity on critical national infrastructure in the region, especially in South Korea.

Overall, the methods employed by North Korea in its offensive cyber operations, and their level of sophistication, are largely indistinguishable from those of cyber criminals. These include using and adapting capabilities developed by others: the attack on Sony Pictures used a variation of Iran's Shamoon wiper capability,

while WannaCry was based on a capability leaked from a US intelligence agency. There is widespread detection and attribution of North Korean cyber activity by Western cyber-security companies.

North Korea's cyber options in a major conflict would therefore be limited, and it certainly lacks the sort of cyber-intelligence reach that would allow it to penetrate and disrupt hardened networks. If tensions rise on the Korean Peninsula, as they did in 2010, the intensity of North Korean cyber operations is likely to increase. Perhaps the greatest danger is that, either intentionally or by miscalculation, such operations would cross the threshold that separates virtual and financial impacts from physical damage.

Notes

1 See Ji Young Kong, Jong In Lim and Kyoung Gon Kim, 'The All-Purpose Sword: North Korea's Cyber Operations and Strategies', in T. Minárik et al. (eds), *11th International Conference on Cyber Conflict: Silent Battle* (Tallinn: NATO CCDCOE Publications, 2019), pp. 1–20, https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf.

2 *Ibid*., p. 1.

3 *Ibid*., p. 2.

4 US Department of Defense, 'Military and Security Developments Involving the Democratic People's Republic of Korea: Annual Report to Congress, Washington DC', 2012, https://archive.defense.gov/pubs/Report_to_Congress_on_Military_and_Security_Developments_Involving_the_DPRK.pdf.

5 Jenny Jun, 'Cyber Coercion: Insights from North Korea's Cyber Campaigns', unpublished paper, 2020, p. 1.

6 *Ibid*., pp. 6–7.

7 Edgar Alvarez, 'Sony Pictures Hack: The Whole Story', Engadget, 10 December 2014, https://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story.

8 United Nations Security Council, 'Report of the Panel of Experts established pursuant to resolution 1874 (2009), S/2019/691', 30 August 2019, pp. 2, 26, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf.

9 United States US-CERT, 'North Korea Threat Advisory', jointly with the Department of State, the Department of Justice and the Federal Bureau of Investigation, 15 April 2020, p. 3, https://us-cert.cisa.gov/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf.

10 UN Sanctions Committee, 'Report of the Panel of Experts established pursuant to resolution 1874 (2009), S/2020/151', United Nations Security Council, 2 March 2020, https://undocs.org/S/2020/151.

11 Jenny Jun, Scott LaFoy and Ethan Sohn, *North Korea's Cyber Operations* (Washington DC: Center for Strategic and International Studies, 2016), https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations.

12 In-bum Chun, 'North Korea's Military Strategy', Korea Economic Institute of America, Washington DC, 2018, http://www.keia.org/publication/north-korea%E2%80%99s-military-strategy-2018.

13 Headquarters, Department of the Army, 'North Korean Tactics', 2020, p. E-1, https://fas.org/irp/doddir/army/atp7-100-2.pdf. 'Unit' is one of the possible translations of the Korean word *gug*; alternatives include 'bureau' and 'station'.

14 'North Korean Cyber Activity', Recorded Future, 2017, p. 6, https://go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf.

15 Kong, Lim and Kim, 'The All-Purpose Sword', p. 6, citing Moonbeom Park, 'Let's learn about enemy through various IoCs of real APT cases', In DragonCon 2018, 8 December 2018, Dragon Threat Labs.

16 *Ibid*., p. 6, citing Mok Yongjae, '6 Cyber Units were built after Kim Jong-un regime', RFA, 22 November 2017.

17 *Ibid*., p. 6, citing Matthew Ha and David Maxwell, 'Kim Jong Un's "All-Purpose Sword" – North Korean Cyber-Enabled Economic Warfare', Foundation for Defense of Democracies, October 2018, p. 13, https://www.fdd.org/wp-content/uploads/2018/09/REPORT_NorthKorea_CEEW.pdf.

18 'APT 37 (Reaper): The Overlooked North Korean Actor', FireEye, 2018, https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf.

19 'APT 38: Un-usual suspects', FireEye, p. 22, https://content.fireeye.com/apt/rpt-apt38.

20 *Ibid*.

21 *Ibid*., pp. 6–8.

22 US Department of State et al., 'Guidance on the North Korean Cyber Threat', 15 April 2020, p. 2, https://us-cert.

cisa.gov/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf.

23 HP Security Research, 'Profiling an enigma: The mystery of North Korea's cyber threat landscape, 2014', HP Security Briefing Episode 16, August 2014, https://time.com/wp-content/uploads/2014/12/hpsr_securitybriefing_episode16_northkorea.pdf; and Department of the Army, 'North Korean Tactics', p. E-1.

24 'Bae saibeo jeonsa 6,800myeong … yeongjaehaggyoseo haekeo yugseong', Yunhap News, 18 February 2021, https://www.yna.co.kr/view/MYH20210218017300038.

25 Jason Bartlett, 'Why Is North Korea So Good at Cybercrime?', *Diplomat*, 13 November 2020, https://thediplomat.com/2020/11/why-is-north-korea-so-good-at-cybercrime.

26 Pratik Jakhar, 'North Korea's high-tech pursuits: Propaganda or progress?', BBC News, 15 December 2018, https://www.bbc.com/news/world-asia-46563454.

27 Ellen Nakashima, Gerry Shih and John Hudson, 'Leaked documents reveal Huawei's secret operations to build North Korea's wireless network', *Washington Post*, 22 July 2019, https://www.washingtonpost.com/world/national-security/leaked-documents-reveal-huaweis-secret-operations-to-build-north-koreas-wireless-network/2019/07/22/583430fe-8d12-11e9-adf3-f70f78c156e8_story.html.

28 Martyn Williams, 'North Korea's Koryolink: Built for Surveillance and Control', 38 North, 22 July 2019, https://www.38north.org/2019/07/mwilliams072219.

29 'ICT in N. Korea 2', KBS World Radio, 31 January 2019, https://world.kbs.co.kr/service/contents_view.htm?lang=e&menu_cate=northkorea&id=&board_seq=356891&page=6&board_code=korea_closeup.

30 Williams, 'North Korea's Koryolink: Built for Surveillance and Control'.

31 Kim Ji-eun and Noh Ji-won, 'North Korea's Smartphone Industry Rapidly on the Rise', HanKyoreh, 17 March 2019, http://english.hani.co.kr/arti/english_edition/e_northkorea/886255.html.

32 'How North Korea Revolutionized the Internet as a Tool for Rogue Regimes', Recorded Future, 9 February 2020, p. 5, https://go.recordedfuture.com/hubfs/reports/cta-2020-0209.pdf.

33 *Ibid*.

34 Insikt Group, 'Shifting Patterns in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite', Recorded Future, 25 October 2018, https://go.recordedfuture.com/hubfs/reports/cta-2018-1025.pdf.

35 David E. Sanger, 'North Korea's Internet Use Surges, Thwarting Sanctions and Fueling Theft', *New York Times*, 11 June 2020, https://www.nytimes.com/2020/02/09/us/politics/north-korea-internet-sanctions.html.

36 Joel Gunter, 'Analysis of North Korea's computer system reveals spy files', BBC News, 28 December 2015, https://www.bbc.com/news/world-asia-35188570.

37 Mun Dong Hui, 'North Korean web developers still in business in China despite lower numbers', Daily NK, 19 April 2019, https://www.dailynk.com/english/north-korean-web-developers-still-in-business-in-china-despite-lower-numbers.

38 Priscilla Moriuchi and Fred Wolens, 'North Korea Relies on American Technology for Internet Operations', Insikt Group, 2018, https://go.recordedfuture.com/hubfs/reports/cta-2018-0606.pdf.

39 See also Martyn Williams, 'Kim Chaek University ranks 8th in international programming contest', North Korea Tech, 4 May 2019, https://www.northkoreatech.org/2019/05/04/kim-chaek-university-icpc-2019; and Kelly Kasulis, 'North Korean college coders beat Stanford University in a 2016 competition. Here's why that matters', Mic, 4 December 2017, https://www.mic.com/articles/186412/north-korean-college-coders-beat-stanford-university-in-a-2016-competition-heres-why-that-matters.

40 Koichiro Komiyama, 'The Information Technology Industry in North Korea', KGRI Working Papers, no. 4, February 2019, p. 5, Keio University Global Research Institute, https://www.kgri.keio.ac.jp/docs/S1806201902 26.pdf.

41 See also Hui, 'North Korean web developers still in business in China despite lower numbers'.

42 Andrea Berger et al., 'The Shadow Sector: North Korea's Information Technology Networks', CNS Occasional Paper, no. 36, May 2018, https://www.nonproliferation.org/wp-content/uploads/2018/05/op36-the-shadow-sector.pdf.

43 For details of the successful launches of the satellites *Kwangmyongsong*-3 and *Kwangmyongsong*-4 in 2012 and 2016 respectively, see 'KMS 3-2', NASA Space Science Data and Coordinated Archive, 14 May 2020, https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=2012-072A; and 'KMS4', NASA Space Science Data and Coordinated Archive, 14 May 2020, https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=2016-009A.

44 'Space Threat 2018: North Korea Assessment', CSIS Aerospace, 12 April 2018, https://aerospace.csis.org/space-threat-2018-north-korea.

45 Robert E. McCoy, 'What Are the Real Purposes of Pyongyang's New Satellites?', *Asia Times*, 19 December 2017, https://asiatimes.com/2017/12/real-purposes-pyongyangs-new-satellites.

46 Todd Harrison et al., 'Threat Assessment 2020', CSIS Aerospace, March 2020, p. 36, https://aerospace.csis.org/wp-content/uploads/2020/03/Harrison_SpaceThreatAssessment20_WEB_FINAL-min.pdf#page=52.

47 Bruce Harrison, 'How North Korea Recruits Its Army of Young Hackers', NBC News, 8 December 2017, https://www.nbcnews.com/news/north-korea/how-north-korea-recruits-trains-its-army-hackers-n825521.

48 'NK establishes university named after leader Kim', Yonhap News Agency, 14 October 2020, https://en.yna.co.kr/view/AEN20201014003000325.

49 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 68, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

50 Karen DeYoung, Ellen Nakashima and Emily Rauhala, 'Trump Signed Presidential Directive Ordering Actions to Pressure North Korea', *Washington Post*, 30 September 2017, https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html.

51 'Significant Cyber Incidents Since 2006', Center for Strategic and International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/210129_Significant_Cyber_Events.pdf.

52 Yashwant Raj, 'North Korea suffers internet blackout after Sony hack', *Hindustan Times*, 24 December 2014, https://www.hindustantimes.com/world/north-korea-suffers-internet-blackout-after-sony-hack/story-Iz7HFvyAPyWaYHd1Zqj52I.html.

53 US Department of Defense, 'Summary Department of Defense Cyber Strategy 2018', September 2018, pp. 1–2, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

54 'Alert (AA20-106A): Guidance on the North Korean Cyber Threat', Cybersecurity and Infrastructure Security Agency, 15 April 2020 (revised 23 June 2020), https://us-cert.cisa.gov/ncas/alerts/aa20-106a.

12. India

Despite the geostrategic instability of its region and a keen awareness of the cyber threat it faces, India has made only modest progress in developing its policy and doctrine for cyberspace security. Its approach towards institutional reform of cyber governance has been slow and incremental, with the key coordinating authorities for cyber security in the civil and military domains only established in 2018 and 2019 respectively. They work closely with the main cyber-intelligence agency, the National Technical Research Organisation. India has a good regional cyber-intelligence reach but relies on partners, including the United States, for wider insight. The strengths of the Indian digital economy include a vibrant start-up culture and a very large talent pool. The private sector has moved more quickly than the government in promoting national cyber security. The country is active and visible in cyber diplomacy but has not been among the leaders on global norms, preferring instead to make productive practical arrangements with key states. From the little evidence available on India's offensive cyber capability, it is safe to assume it is Pakistan-focused and regionally effective. Overall, India is a third-tier cyber power whose best chance of progressing to the second tier is by harnessing its great digital-industrial potential and adopting a whole-of-society approach to improving its cyber security.

Strategy and doctrine

The main lines of India's current approach can be found in ministerial speeches and in government regulations or legislation, rather than in policy documents. In 2013, however, the Ministry of Communications and Information Technology did release the country's first National Cyber Security Policy,[1] a short document affirming the need to protect the government, businesses and citizens from cyber attacks either by state or non-state actors. It presented basic recommendations for government organisations and private companies, including the allocation of budgets and personnel for cyber-security purposes and the drafting of information-security policies. It also set out national objectives, including the training of 500,000 cyber-security professionals over the following five years, the development of indigenous cyber-security technologies, the establishment of public–private partnerships, and the promotion of a culture of cyber security and privacy that would encourage responsible behaviour by internet users.

India's thinking on cyber policy for the civil sector continues to develop. Government officials had planned to issue a new national cyber-security strategy in 2020

List of acronyms

CERT-In	Computer Emergency Response Team India
DCA	Defence Cyber Agency
DIA	Defence Intelligence Agency
DSCI	Data Security Council of India
IB	Intelligence Bureau
ICT	information and communications technology
NCCC	National Cyber Coordination Centre
NCIIPC	National Critical Information Infrastructure Protection Centre
NTRO	National Technical Research Organisation
RAW	Research and Analysis Wing

to address developments in 5G, ransomware and the Internet of Things.[2] That effort appears to have stalled but the government is actively reframing all areas of cyber-security policy, including education, skills, import controls and national security. The military confrontation with China in the disputed Ladakh border area in June 2020, followed by a sharp increase in Chinese activity against Indian networks, has heightened Indian concerns about cyber security, not least in systems supplied by China. In a speech on Independence Day in August 2020, Prime Minister Narendra Modi devoted a paragraph to the new cyber-security strategy, promising it would soon emerge.[3] In January 2021 a high-level government meeting was held to discuss a security strategy for the telecoms sector.[4] Key planks of India's cyber-security policy will probably align quite closely with the priorities laid out in a consultation paper released by the Data Security Council of India (DSCI), the principal private-sector organisation in the field.[5] The paper addresses 21 different areas of policy while depicting a backdrop of increasing threats and, in the opinion of the DSCI, insufficient government action.

As for the approach taken by India's armed forces, in 2017 they publicly released a joint doctrine in which cyberspace, though subsumed under the rubric of information warfare, was afforded a prominent role.[6] Placing strong emphasis on the integration of capabilities across the armed forces, cyber power – defined as 'the ability to use cyberspace freely and securely to gain an advantage over the adversary while denying the same to him in various operational environments' – was presented as equal in importance to land, sea, air and space power and special-forces operations. Treating cyber capabilities as one of a triad of integrated strategic forces alongside space and special operations, the doctrine presaged the establishment of a Defence Cyber Agency, eventually created in 2019. It also emphasised the importance of cyber security for India's economy and critical national infrastructure, placing the defence of the country's cyberspace on a par with the defence of its territory, airspace and trade routes. Moreover, the doctrine identified cyber warfare as a component of hybrid warfare, which it described as a key element in 'current fifth generation war' (though there was no clear definition of hybrid warfare or fifth-generation war from India's perspective).

Cyber capabilities also featured prominently in the new Land Warfare Doctrine released by the Indian Army in late 2018.[7] Again subsumed within information warfare, cyberspace was designated as a new dimension of warfare and an important factor in winning future battles. The document foreshadowed the increasing integration of cyber capabilities into the conventional and sub-conventional realms, including for covert operations. In it, the army set itself the task not only of developing or upgrading cyber-deterrence and cyber-defence capabilities, but also of retaining the capability to fight in the face of prolonged attempts at cyber disruption.

Governance, command and control

India's cyber command-and-control structure has been under development since the early 2000s but remains decentralised. Cyber-security powers are spread across a number of agencies, with reports of overlapping competencies and bureaucratic turf wars.[8] The situation is further complicated by the country's federal political structure. Several key institutions were set up between 2004 and 2008, all operating under the direction of ministers and coming together in the National Security Council of the Cabinet, which sits at the apex of security decision-making. The main cyber agency, the National Technical Research Organisation (NTRO), set up in 2004 and modelled on the US National Security Agency, reports to the national security advisor and is tasked with technical intelligence-gathering, signals interception and influence operations.[9] A National Information Board, responsible for information security, was established in 2004 as an advisory committee, in part to formulate a national policy on information warfare.[10] In 2003 the government set up a national Computer Emergency Response Team (CERT-In) which operates under the Ministry of Electronics and Information Technology.

In 2008, amendments to the Information Technology Act of 2000 gave government agencies wide-ranging powers to 'issue directions for interception, monitoring or decryption of any information through any computer resource'.[11] The legislation also sought protections for 'critical information infrastructure' networks. It was also in 2008 that the main private-sector body representing the ICT sector, the National

Association of Software and Service Companies, set up the DSCI, which has proved an effective advocate in mobilising more effective government responses in the area of cyber security.

A security review in 2011–12, ordered by the prime minister, identified cyber security as a key area of development and recommended the establishment of a centralised cyber command and analogous civilian entities with oversight powers across government agencies.[12]

By 2013, following allegations about cyber espionage conducted against India by several countries (including the United States and China) and leaks concerning India's own offensive cyber capabilities, the government was keenly aware of the need for improved policy and action. However, institutional development over the next few years was quite piecemeal. A National Critical Information Infrastructure Protection Centre (NCIIPC) was established in 2014 under the direction of the NTRO.[13] A National Cyber Coordination Centre (NCCC), subordinate to CERT-In, finally began operations in 2018 (having first received ministerial approval in 2013). The NCCC is responsible for intelligence-sharing between government agencies and for coordinating government responses to cyber attacks.[14]

The Defence Cyber Agency (DCA), created in 2019, is central to the command and control of India's military cyber capabilities. Its intended role is to integrate and coordinate the cyber, space and special-forces capabilities of the three armed services. It is part of the Integrated Defence Staff, a tri-service headquarters which includes civilian representation from the Ministry of External Affairs and other ministries. It comprises a sizeable tri-service staff of about 1,000, divided into several teams based at a command centre in Delhi and in other locations around the country.[15] By operationalising the 2017 joint doctrine's focus on capability integration, the DCA represents both an important institutional evolution and a significant maturing of India's approach to military uses of cyberspace.

Core cyber-intelligence capability

India's intelligence priorities are deeply shaped by internal and external terrorist threats, internal political violence and the ongoing conflict with Pakistan over Kashmir. The internally focused Intelligence Bureau (IB) is responsible for counter-terrorism and counter-intelligence, in cooperation with the state police and national paramilitary forces.[16] India's foreign intelligence agency is the Research and Analysis Wing (RAW). The Defence Intelligence Agency (DIA), created in 2002, now coordinates all defence-intelligence assets, including the Signals Intelligence Directorate and the DCA. Intelligence collection by these three main agencies is digitally enabled via a real-time intelligence grid (NATGRID) that links citizen-data sources across multiple government and private databases to facilitate the monitoring of terrorist activities that pose a threat to banking, finance and transportation networks. In addition, the IB and RAW are empowered to monitor internet traffic through a system enabling the interception of internet communications, including social media.[17] While the IB, RAW and DIA each represent a part of India's cyber-intelligence capability, they are all heavily reliant for core capability on the technical-intelligence agency, the NTRO. Various parts of the Ministry of Home Affairs, including the Cyber Crime Wing and Central Forensics Science Laboratory, are also important sources of cyber intelligence.

Beyond the domestic threats, India's cyber-intelligence capabilities have unsurprisingly been focused on its near abroad, particularly Pakistan

Beyond the domestic threats, India's cyber-intelligence capabilities have unsurprisingly been focused on its near abroad, particularly Pakistan. For example, there are indications that, since about 2010, Indian cyber teams have been targeting IP addresses in Pakistan (and to a lesser extent in China), as well as secessionist movements within India itself, in a significant cyber-surveillance and cyber-espionage operation.[18] Further afield, however, India's cyber-intelligence reach appears weak: it tends to rely on partnerships such as those with the US, the United Kingdom and France for a higher level of cyber

situational awareness and to help it develop a greater reach of its own in future.

Mirroring the UK, the Indian government has set up a Joint Intelligence Committee attached to the office of the prime minister, tasked with collecting, assessing and prioritising inputs from all the country's intelligence agencies.[19] A Multi-Agency Centre (MAC) has also been established under the IB, together with subsidiary MACs in different states, with the aim of enhancing the sharing of information between intelligence units, including finance and defence ministries at the state and national levels.

Cyber empowerment and dependence

India is an ICT powerhouse, with a digital economy estimated in value at US$190 billion[20] and a tech start-up sector assessed to be the third largest in the world.[21] According to one estimate, core digital sectors such as ICT-enabled services and electronics manufacturing will contribute around 10% of GDP by 2025.[22] However, only slightly more than half of India's 1.4bn people have access to the internet, and the levels of mobile-phone ownership and internet use are far higher among men than women.[23] Most Indians who access the internet do so by mobile phone, though download speeds are below the global average. Agriculture, which still provides the livelihoods of hundreds of millions of Indians, is undergoing some digitisation and employing tools and techniques that rely on automated and autonomous machines. However, the vast majority of the population (about 90%) lack basic digital skills.[24] As one way of addressing the issue, the government has been increasing the availability of apps and digital services in a greater number of local languages.

Foreign investment plays a large part in India's digital economy, with the country providing outsourced IT services around the world and serving as a major production hub for global brands, such as Dell computers. From 2014 to 2020, US ICT investment totalled US$30bn and Japanese investment US$12bn.[25] As for Chinese ICT investment, it surpassed US$4bn in the same period, with Alibaba and Tencent accounting for three-quarters of the total.[26]

The infrastructure at the heart of India's digital economy is built largely from imported equipment – for example, four of the top five mobile devices by market share are manufactured by Chinese companies.[27] Almost all the country's most popular mobile apps – such as Facebook Messenger, PlayerUnknown's Battlegrounds (PUBG), SHAREit, TikTok (at least until India's ban on Chinese apps in 2020), Truecaller, UC Browser and WhatsApp – were designed abroad. One exception, in 2020, was Aarogya Setu, the Indian government's COVID-19 contact-tracing app. As a result, and despite breakthroughs by Indian companies in app development and plans to develop 5G systems, the government has limited agency over the way in which devices and platforms manage the flow of data through their systems.

In the field of artificial intelligence (AI), India's research capability has been placed quite highly in global rankings, achieving ninth[28] and 13th[29] position, for example, in two authoritative studies. The lion's share of AI research and development (about 85%) is conducted by universities rather than industry.[30] The Indian Institute of Technology (IIT) Hyderabad has collaborated with Nvidia, an American multinational technology company, to establish India's first AI Technology Centre, aimed at accelerating research and its commercial adoption.[31] The centre intends to focus on advanced AI research in areas of agriculture, smart cities and language-understanding, in line with the priorities stated in India's national strategy for AI.[32] In terms of the application of AI to industrial processes, it is notable that India was ranked third, after the US and China, in a 2018 study by the Boston Consulting Group.[33] The country's AI start-ups received total investment of US$762m in 2019, a 44% increase in comparison with 2018.[34]

The space industry is led by the Indian Space Research Organisation (ISRO), which is one of the world's six largest space agencies and owns one of the largest fleets of communication and remote-sensing satellites used for civil and military purposes.[35] ISRO also operates satellites for surveillance and navigation purposes – including the Indian Regional Navigation Satellite System;[36] dual-use surveillance satellites in the Cartostat and RISAT series;[37] and EMISAT, launched in 2019, which can detect an adversary's electromagnetic signals.[38] Owing to capacity limitations in its own agencies,[39] the Indian government has begun to rely

more on commercial enterprises to develop and produce space equipment such as satellites and propulsion systems. Like many other countries, India still relies on foreign suppliers for the space sector, with Hughes Communications India appointed to provide a high-performance satellite broadband system for India's Naval Communication Network.[40] It has, however, achieved self-reliance in the production of launch vehicles and some satellite technologies.[41]

A unique characteristic of the Indian cyber economy is the huge number of graduates in ICT-related subjects entering the job market every year: in 2019 the figure was almost 600,000, which was five times more than in the US.[42]

Cyber security and resilience

India's state administrations have numerous cyber-security-related offices with large numbers of staff, and much attention has been paid to cyber crime since 2009, when the country became one of the first to introduce cyber-crime courts and cyber police stations. But perhaps the most distinctive feature of India's cyber-security infrastructure is the importance of the private sector, which has led the way in developing strong policies and standards. The rapid integration of the internet into everyday economic life, albeit from a low base, has created the need for new cyber-security capabilities on a scale and at a pace unseen in any other country – hundreds of millions of Indians have begun to participate in e-commerce in the last five years, for example.[43] The main challenges lie in policy coordination, ensuring consistency around the country, and addressing the general lack of depth in cyber-security skills relative to the size of the population and the needs of industry.

India has frequently been the victim of cyber attacks, including on its critical infrastructure, and has attributed a significant proportion of them to China or Pakistan. CERT-In reported, for example, that there were more than 394,499 incidents in 2019,[44] and 2020 saw an upsurge in attacks from China.[45] Of particular concern to the Indian government are cyber attacks by North Korea that use Chinese digital infrastructure.[46] The vast majority of the cyber incidents flagged by CERT-In appear to have been attempts at espionage,[47] but they could also have resulted in serious damage to the integrity of Indian networks and platforms. In 2020, India had the second-highest incidence of ransomware attacks in the world[48] and the government banned 117 Chinese mobile applications because of security concerns.[49]

India regards its financial institutions as particularly vulnerable to cyber attack.[50] In August 2018, in a persistent attack on Cosmos Bank by a North Korean group, US$13.5m was siphoned off from customers' accounts.[51] A United Nations Security Council panel of experts, appointed to study North Korea's attempts to evade UN sanctions, suggested in a July 2019 report that Indian banks may have been the victims of cyber theft by North Korea amounting to nearly US$200m over a three-year period.[52] On the other hand, thanks to stringent guidelines from the Reserve Bank of India (RBI), the financial sector is more secure than other areas of the Indian economy. For example, two-factor authentication, strictly audited by the RBI, is the norm in internet banking and e-commerce.[53]

Although India's central government has been slow in addressing cyber security, the private sector has been far more active and more effective. The DSCI, which promotes best practices and standards for cyber security and privacy, undertakes capacity-building projects with a focus on training and certification, including for the government sector. In 2020 it said there was a 'dire need' for the government to play its part in promoting cyber security in the country, and recommended a quadrupling of government expenditure on cyber security as the country's digital economy expands.[54] India was ranked 47th out of 175 countries in the International Telecommunication Union's 2018 Global Cybersecurity Index, well behind its geopolitical rival China (27th).[55]

In cyber-resilience policy and preparedness for emergencies, India has some foundations in place, with the NCIIPC active in promoting policies and procedures throughout the country since it was created in 2014. Progress in emergency-response planning has in many cases been slower at the state level, with Tamil Nadu, for example, only introducing a cyber-security strategy in 2020.[56] In contrast, the state of Maharashtra, which contains the commercial and financial hub of Mumbai, has a well-established cyber-security team in its police force and dedicated cyber 'police stations' in various parts of Mumbai.

However, compared with equivalent bodies in some wealthier countries, the NCIIPC is not well equipped to handle cyber emergencies and wider resilience-planning – for example, as of 2018, there was only one sector (power) where it had been able to organise stakeholders around those objectives.[57] There are also indications that the NCIIPC has not coordinated well with other government bodies.[58] It is unclear, for example, if steps have been taken to improve cyber defences at the Unique Identification Authority of India, after its database of citizens' biometric information (the second-largest in the world) was reported to have been breached in 2017, or the Kudankulam Nuclear Power Plant, which in 2019 was the target of a serious cyber attack that it initially denied and then downplayed.[59] In Maharashtra, where the power sector was targeted by Chinese hackers (dubbed the Red Echo group) from early 2020, it seems the cyber-security department in the state police were informed of the threat by CERT-In in November 2020 but the NCIIPC only alerted the Ministry of Power on 12 February 2021.[60]

Though the National Cyber Security Coordinator conducts periodic whole-of-government audits involving relevant agencies, the government has faced an uphill battle in trying to make new entities such as the NCIIPC work seamlessly alongside long-established public-sector bodies that are in various stages of digitising their infrastructure. The NCIIPC has taken private enterprises under its wing, including oil and gas companies, and tries to ensure that the public and private sectors work in tandem on cyber security.

The first reported cyber exercise in the Indian Armed Forces, *CyberEx*, was conducted by the Indian Defence University on 29–30 April 2019.[61] It involved the NTRO, the three services, the National Security Council Secretariat, CERT-In, the Defence Research and Development Organisation, the National Informatics Centre, academia and industry.

Global leadership in cyberspace affairs

As a nuclear power with large conventional forces, a burgeoning digital economy and a determination to increase its geopolitical influence, India is the target of cyber espionage by a wide range of states. However, it knows its defensive capabilities are relatively weak. As a result, it pursues diplomatic efforts to bring the governance of cyberspace within the rules-based international order, while maintaining a realistic approach to dealing with the states that are targeting its networks.

In its National Cyber Security Policy of 2013, India's diplomatic goals included the development of bilateral and multilateral cyber-security relationships as well as global cooperation between national law-enforcement agencies, security services, judicial systems and armed forces.

Unsurprisingly, the challenges involved in defending its open networks (and largely imported infrastructure) have prompted India to advocate international norms of restraint. It appears to have abandoned its previous opposition to emerging international legal principles such as the possible voluntary norms on security in cyberspace put forward by the UN Group of Governmental Experts (GGE) in 2015.[62] As a member of the 2016–17 GGE, India endorsed the inclusion in the final report of a right to self-defence in cyberspace, although the draft did not receive the unanimous consent of all participating experts.[63] It is unclear whether India will further endorse the right to retaliatory measures for acts that fall below the thresholds that qualify as a 'threat or use of force' or 'armed attack' under international law.

India knows its defensive cyber capabilities are relatively weak

India's most developed bilateral cyber partnership is with the US. The two countries have held a regular cyber dialogue since the early 2000s, intensifying in 2015 with the decision to convene a 'Track 1.5' programme that seeks to convene government officials and business leaders to collaborate on cyber questions. Cyber is also envisioned as a component of several other US–India agreements, including on intelligence-sharing and mutual legal assistance.[64]

India has also pursued bilateral cyber dialogues with several other partners, including the European Union, Russia and the UK. The cyber partnership with the UK is particularly well developed, with a regular dialogue dating back to 2012. In April 2018 the two countries

signed a framework agreement identifying avenues for bilateral cooperation on cyber security and establishing working groups on cyber diplomacy, cyber crime, incident response and the digital economy.[65] They have also agreed in principle to establish a joint Cyber Security Training Centre of Excellence.[66]

Offensive cyber capability

Public statements by Indian officials and other open-source material indicate that India has developed relatively advanced offensive cyber capabilities focused on Pakistan. It is now in the process of expanding these capabilities for wider effect.

India reportedly considered a cyber response against Pakistan in the aftermath of the November 2008 terrorist attacks in Mumbai, with the NTRO apparently at the forefront of deliberations.[67] A former national security advisor has since indicated publicly that India possesses considerable capacity to conduct cyber-sabotage operations against Pakistan,[68] which appears credible.

It is difficult to gauge the extent or orientation of India's current investment in offensive capabilities but there are some indications that the focus may have shifted more to countering China, given its growing economy and regional power.[69] There is also evidence dating back to 2014 of Prime Minister Modi's interest in creating a 'Digital Armed Force', in part for deterrent purposes.[70] A 2019 report commissioned by an influential Indian think tank with close links to the ruling Bharatiya Janata Party urged the rapid development of offensive cyber capabilities but cautioned against any public declaration until those capabilities were in place.[71]

Overall, India's focus on Pakistan will have given it useful operational experience and some viable regional offensive cyber capabilities. It will need to expand its cyber-intelligence reach to be able to deliver sophisticated offensive effect further afield, but its close collaboration with international partners, especially the US, will help it in that regard.

Notes

1 Ministry of Communications and Information Technology, 'National Cyber Security Policy 2013', 2 July 2013, https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.

2 Aditi Agrawal, 'India's cybersecurity strategy policy in 2020, says National Cybersecurity Coordinator Rajesh Pant', Medianama, 22 June 2019, https://www.medianama.com/2019/06/223-indias-cybersecurity-strategy-policy-in-2020-says-national-cybersecurity-coordinator-rajesh-pant.

3 Elizabeth Roche, 'PM Modi says India to have new cyber security policy soon', Livemint, 15 August 2020, https://www.livemint.com/news/india/pm-modi-says-india-to-soon-have-cyber-security-policy-11597461750194.html.

4 'Govt formulating new action plan, Chinese telecom giants could be out of game', *Economic Times*, 21 January 2021, https://telecom.economictimes.indiatimes.com/news/govt-formulating-new-action-plan-chinese-telecom-giants-could-be-out-of-game/80391251.

5 Data Security Council of India, 'National Cyber Security Strategy 2020: DSCI submission', 2020, https://www.dsci.in/sites/default/files/documents/resource_centre/National%20Cyber%20Security%20Strategy%202020%20DSCI%20submission.pdf.

6 Headquarters Integrated Defence Staff, Ministry of Defence, 'Joint Doctrine – Indian Armed Forces', 2017, https://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf.

7 Indian Army, 'Land Warfare Doctrine 2018', http://www.ssri-j.com/MediaReport/DocumentIndianArmyLandWarfareDoctrine2018.pdf.

8 Tarun Krishnakumar, 'Cyber Insecurity: Regulating the Indian Financial Sector', Oxford University Faculty of Law, 21 August 2017, https://www.law.ox.ac.uk/business-law-blog/blog/2017/08/cyber-insecurity-regulating-indian-financial-sector.

9 B. Raman, 'Possible Misuse of New TECHINT Capabilities', *Indian Defence Review*, 5 December 2011, http://www.indiandefencereview.com/spotlights/possible-misuse-of-new-techint-capabilities.

10 Saikat Datta, 'Low on the IQ', *Outlook*, 4 July 2005, https://magazine.outlookindia.com/story/low-on-the-iq/227823.

11 'Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009', The Centre for Internet & Society, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.

12 Vinod Anand, 'Defence Reforms and Naresh Chandra Task Force Review', Vivekananda International Foundation, 13 September 2012, https://www.vifindia.org/article/2012/september/13/defence-reforms-and-naresh-chandra-task-force-review.

13 Government of India, National Technical Research Organisation, https://ntro.gov.in/welcome.do.

14 'India now has a National Cyber Coordination Centre (NCCC) to monitor cyber threats', India Today, 11 August 2007, https://www.indiatoday.in/education-today/gk-current-affairs/story/nccc-cyber-india-1029203-2017-08-11.

15 Rahul Bedi, 'India setting up tri-service commands for special forces, cyber security, and space', *Jane's Defence Weekly*, 16 May 2019.

16 See Mahendra Kumawat and Vinay Kaura, 'Building the resilience of India's internal security apparatus', Observer Research Foundation, Occasional Paper 176, November 2018, https://www.orfonline.org/wp-content/uploads/2018/11/ORF_OccasionalPaper_176_Security_NEWFinalPDF.pdf.

17 See Udbhav Tiwari, 'The Design & Technology Behind India's Surveillance Programmes', The Centre for Internet & Society, 20 January 2017, https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes#_ftnref13.

18 Snorre Fagerland et al., 'Operation Hangover: Unveiling an Indian Cyber Attack Infrastructure', Norman Shark, May 2013, http://docshare.tips/unveiling-an-indian-cyberattack-infrastructure_58a3ff6db6d87f499c8b462d.html.

19 See Musa Tuzuner (ed.), *Intelligence Cooperation Practices in the 21st Century: Towards a Culture of Sharing* (Amsterdam: IOS Press, 2010).

20 'How the IT sector has emerged as a pillar of modern India', *Hindu*, 14 August 2020, https://www.thehindubusinessline.com/news/national/how-the-it-sector-has-emerged-as-a-pillar-of-modern-india/article32357389.ece. This estimate is based on a classic narrow view of the ICT sector, as usually reported in national accounts. However, the Organisation for Economic Co-operation and Development and other research institutions have been adopting a definition of the digital economy based on a broader set of indicators. According to one of these broader estimates, India's digital economy was worth US$570bn in 2019, equivalent to about 20% of GDP.

21 Trisha Ray et al., *The Digital Indo-Pacific: Regional Connectivity and Resilience*, The Australian Government for the Quad Tech Network, February 2021, p. 8, https://www.orfonline.org/wp-content/uploads/2021/02/thedigitalindopacific.pdf.

22 McKinsey Global Institute, 'Digital India: Technology to Transform a Connected Nation', March 2019, https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20nation/digital-india-technology-to-transform-a-connected-nation-full-report.ashx.

23 Romita Majundar, 'Gender gap in mobile and internet usage in India as per GSMA report', *Business Standard*, 9 March 2019, https://www.business-standard.com/article/economy-policy/gender-gap-in-mobile-and-internet-usage-in-india-as-per-gsma-report-119030900696_1.html.

24 Digital Empowerment Foundation, 'About', undated, https://www.defindia.org/national-digital-literacy-mission.

25 Ray et al., *The Digital Indo-Pacific: Regional Connectivity and Resilience*, p. 9.

26 *Ibid*.

27 Sam Byford, 'Realme Takes Chunk of India Mobile Market as Samsung Slides', The Verge, 11 November 2019, https://www.theverge.com/2019/11/11/20958932/india-mobile-marketshare-q3-2019-idc-realme-samsung-xiaomi.

28 JJiqiang Niu et al., 'Global research on artificial intelligence from 1990–2014: Spatially-explicit bibliometric analysis', *ISPRS International Journal of Geo-Information*, vol. 5, no. 5, p. 8, https://www.mdpi.com/2220-9964/5/5/66/pdf.

29 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.

30 Richa Bhatia, 'Where Artificial Intelligence Research in India Is Heading', Analytics India Magazine blog, 27 March 2018, https://analyticsindiamag.com/where-artificial-intelligence-research-in-india-is-heading.

31 Anisha Kumari, 'IIT Hyderabad, NVIDIA Establish First AI Research Centre in India', NDTV, 9 July 2020, https://www.ndtv.com/education/iit-hyderabad-nvidia-establish-first-ai-research-centre-in-india.

32 Canadian Institute for Advanced Research, 'Building an AI World: Report on National and Regional AI Strategies Second Edition', May 2020, p. 22, https://cifar.ca/wp-content/uploads/2020/10/building-an-ai-world-second-edition.pdf.

33 'India Ranked Third in Terms of Artificial Intelligence Implementation: Report – ET CIO', ETCIO, 26 April 2018, https://cio.economictimes.indiatimes.com/news/business-analytics/india-ranked-third-in-terms-of-artificial-intelligence-implementation-report/63922875.

34 AIMResearch, 'Report: Indian AI Startup Funding in 2019', 28 January 2020, p. 4, https://analyticsindiamag.com/report-indian-ai-startup-funding-in-2019.

35 Indian Space Research Organisation, 'About ISRO', https://www.isro.gov.in/about-isro.

36 The Indian Regional Navigation System Satellite is made up of seven satellites that serve civil purposes but also provide encrypted data to the Indian armed forces. See G.D. Sharma, *Exploiting Indian Military Capacity in Outer Space* (New Delhi: Centre for Joint Warfare Studies, 2016), https://cenjows.in/pdf/issue/Layout_Exploiting%20Indian%20Military.pdf.

37 See Government of India, Department of Space, Indian Space Research Organisation, 'List of Earth Observation Satellites', https://www.isro.gov.in/spacecraft/list-of-earth-observation-satellites.

38 Manu Pubby, 'Navy to Buy Rs 1,589 Crore Satellite From ISRO', *Economic Times*, 18 July 2019, https://economictimes.indiatimes.com/news/defence/navy-to-buy-rs-1589-crore-satellite-from-isro/articleshow/70283927.cms?from=mdr.

39 Narayan Prasad Nagendra and Prateep Basu, 'Demystifying Space Business in India and Issues for the Development of a Globally Competitive Private Space Industry', *Space Policy*, vol. 36, 2016, pp. 1–11, https://www.sciencedirect.com/science/article/abs/pii/S0265964616300078.

40 John Sheldon, 'Indian Military Space: Hughes India and Sterlite Tech Enable Satcom Connectivity for Indian Navy', Spacewatch, January 2019, https://spacewatch.global/2019/01/indian-military-space-hughes-india-and-sterlite-tech-enable-satcom-connectivity-for-indian-navy.

41 Rajeswari Pillai Rajagopalan, Pulkit Mohan and Rahul Krishna, 'India in the Final Frontier: Strategy, Policy and Industry', ORF Special Report no. 100, Observer Research Foundation, 29 January 2020, https://www.orfonline.org/research/india-in-the-final-frontier-strategy-policy-and-industry-60834.

42 Organisation for Economic Co-operation and Development, *Measuring the Digital Transformation*: *A Roadmap for the Future* (Paris: OECD Publishing, 2019), p. 144, https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm.

43 In 2016 the government set up the Unique Identification Authority of India, which provided a new foundation for biometric identification to support more secure electronic banking and e-commerce across the country, especially by mobile phone. While the organisation had been conducting business under another name since 2010 and issuing IDs, there has been an explosion of the process since 2016, with 1.24bn citizens now registered. See Unique Identification Authority of India, 'About UIDAI', https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html.

44 Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, 'CERT-In Annual Report (2019)', p. 3, https://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2020-0001.pdf.

45 Manu Kaushik, '200% rise in cyberattacks from China in a month; India tops hit list post Galwan face-off', *Business Today*, 24 June 2020, https://www.businesstoday.in/technology/news/200-percent-rise-in-cyberattacks-from-china-in-a-month-india-tops-hit-list-post-galwan-face-off/story/407806.html.

46 Interview with former official in the Indian government, New Delhi, 4 October 2019.

47 Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, 'CERT-In Annual Report (2018)', p. 6, https://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2019-0123.pdf.

48 National Critical Information Infrastructure Protection Centre, 'NCIIPC Newsletter', January 2021, p. 2, https://nciipc.gov.in/documents/NCIIPC_Newsletter_Jan21.pdf.

49 'India bans PUBG, 117 other Chinese apps for "stealing, transmitting users' data" to servers outside India', FirstPost, 20 September 2020, https://www.firstpost.com/india/india-bans-pubg-117-other-chinese-apps-for-stealing-transmitting-users-data-to-servers-outside-india-8778561.

50 'Banks Most Vulnerable to Cyber Threats: National Cyber Security Coordinator', *New Indian Express*, 20 February 2019, https://www.newindianexpress.com/business/2019/feb/20/banks-most-vulnerable-to-cyber-threats-national-cyber-security-coordinator-1941363.html.

51 Rashmi Rajput, 'UN Security Council Panel Finds Cosmos Bank Cyber Attack Motivated by N Korea', *Economic Times*, 27 March 2019, https://economictimes.indiatimes.com/industry/banking/finance/banking/un-security-council-panel-finds-cosmos-bank-cyber-attack-motivated-by-n-korea/articleshow/68589549.cms?from=mdr.

52 United Nations Security Council, 'Report of the Panel of Experts established pursuant to Resolution 1874 (2009)', 5 March 2019, S/2019/171, https://www.

securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3CF6E4FF96FF9%7D/s_2019_171.pdf.

53 Reserve Bank of India, 'Master Direction on Digital Payment Security Controls', 18 February 2021, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF.

54 DSCI, 'National Cyber Security Strategy 2020: DSCI submission'.

55 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 58, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

56 Raja Simhan, 'TN govt working on giving the "cyber resilience" edge to governance', The Hindu Business Line, 24 December 2020, https://www.thehindubusinessline.com/info-tech/tn-govt-working-on-giving-the-cyber-resilience-edge-to-governance/article33409737.ece.

57 Munish Sharma and Cherian Samuel, *India's Strategic Options in a Changing Cyberspace* (Delhi: Pentagon Press, 2018), p. 110, https://idsa.in/system/files/book/book_indias-strategic-options-in-cyberspace.pdf.

58 See, for example, Saikat Datta, 'Defending India's Critical Information Infrastructure', Internet Democracy Project, 2016, https://internetdemocracy.in/wp-content/uploads/2016/03/Saikat-Datta-Internet-Democracy-Project-Defending-Indias-CII.pdf; and Shatabdi Mazumder, 'The Need for Re-conditioning of India's Cyber Security', Apeksha News Network, 28 September 2020, https://apekshanews.com/the-need-for-re-conditioning-of-indias-cyber-security.

59 Sushovan Sircar and Vakasha Sachdev, 'Kudankulam Cyber Attack Did Happen, Says NPCIL a Day After Denial', The Quint, 1 November 2019, https://www.thequint.com/news/india/kudankulam-nuclear-power-plant-malware-attack-correct-confirms-npcil.

60 'Chinese cyber attack foiled: Power Ministry', *Hindu*, 1 March 2021, https://www.thehindu.com/news/national/attacks-by-chinese-groups-thwarted-power-ministry/article33965683.ece.

61 Press Information Bureau, 'Cyber Exercise on Scenario Building & Response', 29 April 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=189871.

62 James Crawford, Jacqueline Peel and Simon Olleson, 'The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: Completion of the Second Reading', *European Journal of International Law*, vol. 12, no. 5, 2001, pp. 963–91, http://www.ejil.org/pdfs/12/5/1557.pdf. 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.

63 Interview with a member of the 2016–17 GGE, August 2017.

64 Nayantara Ranganathan, 'Cybersecurity and bilateral ties of India and the United States: A very brief history', Internet Democracy Project, 30 September 2015, https://internetdemocracy.in/reports/cybersecurity-and-india-us-bilateral-ties-a-very-brief-history.

65 Rahul Roy-Chaudhury, 'India–UK cybersecurity cooperation: The way forward', International Institute for Strategic Studies blog, 22 November 2019, https://www.iiss.org/blogs/analysis/2019/11/sasia-india-uk-cyber-security-cooperation.

66 Rahul Roy-Chaudury, 'India–UK cyber security cooperation: The way forward', India Global Business, 15 November 2019, https://www.indiaglobalbusiness.com/igb-archive/india-uk-cyber-security-cooperation-the-way-forward-india-global-business.

67 Raj Chengappa and Sandeep Unnithan, 'How to Punish Pakistan', India Today, 22 September 2016, https://www.indiatoday.in/magazine/cover-story/story/20161003-uri-attack-narendra-modi-pakistan-terror-kashmir-nawaz-sharif-india-vajpayee-829603-2016-09-22.

68 M.K. Narayanan, 'The Best among Limited Options', *Hindu*, 1 November 2016, https://www.thehindu.com/opinion/lead/The-best-among-limited-options/article14990381.ece.

69 Arditi Agrawal, 'India's Cybersecurity Strategy Policy in 2020, Says National Cybersecurity Coordinator Rajesh Pant', Medianama, 22 June 2019, https://www.medianama.com/2019/06/223-indias-cybersecurity-strategy-policy-in-2020-says-national-cybersecurity-coordinator-rajesh-pant.

70 Narendra Modi, 'PM's Address at the Combined Commanders' Conference', 17 October 2014, https://www.narendramodi.in/amp/pms-address-at-the-combined-commanders-conference.

71 Vivekananda International Foundation, 'Credible Cyber Deterrence in Armed Forces of India', March 2019, https://www.vifindia.org/sites/default/files/Credible-Cyber-Deterrence-in-Armed-Forces-of-India_0.pdf.

13. Indonesia

Indonesia's first formal strategy for civil-sector cyber security emerged only in 2018, one year after its principal cyber agency was created. Cyber-related institutional changes within the armed forces began around 2014 but have not yet given rise to a published military cyber strategy or doctrine. Political control of cyber policy is exercised through the president. Indonesia has only limited cyber-intelligence capabilities but has been investing in cyber surveillance for domestic security. It is more engaged than most developing countries in cyber security and in employing digital technologies. On international cyberspace policy, it participates actively in the G20, the Asia-Pacific Economic Cooperation, the Association of Southeast Asian Nations and the Organisation of Islamic Cooperation. Indonesia has some cyber-surveillance and cyber-espionage capabilities, but there is little evidence of it planning for, or having conducted, offensive cyber operations. Overall, Indonesia is a third-tier cyber power. Given that it is expected to become the fourth-largest economy in the world by around 2030, it could be well placed to rise to the second tier if the government decides that strategic circumstances demand greater investment in the cyber domain.

Strategy and doctrine

Until 2017, cyberspace policy in Indonesia was largely undeveloped. Institutions, coordination and legal foundations were all weak and there was no overall national strategy.[1] Only some basic institutional foundations were in place: the National Crypto Agency (founded in 1946) had been strengthened to some extent; a Computer Emergency Response Team (CERT) had been created in 1998 through a private initiative; there was a government infrastructure-incident-response team (another CERT, in practice), set up in 2007;[2] 14 additional CERTs were in place by 2016; and some relevant laws and regulations had been refined.[3]

The principal development in 2017 was the establishment, by presidential decree, of the National Cyber and Crypto Agency (BSSN),[4] replacing the National Crypto Agency.[5] Also in 2017, the national police force announced the expansion of its cyber-crime unit from 40 to 100 personnel.[6] The country began to frame its cyber defence in very broad terms as part of its concept of 'total defence'.[7]

The first national cyber-security strategy was published by the BSSN in 2018, setting out five objectives: cyber resilience, security of public services, enforcement of cyber law, a culture of cyber security, and cyber security in the digital economy.[8] The strategy was also intended to support the country's counter-terrorism policies. Its stated goals included the promotion of multi-stakeholder engagement and fostering global trust in Indonesia's management of its cyberspace. As in most countries, the publication of a formal strategy

List of acronyms

ASEAN	Association of Southeast Asian Nations
BSSN	National Cyber and Crypto Agency
MoD	Ministry of Defence
OIC	Organisation of Islamic Cooperation
TNI	Indonesian Armed Forces

provided a foundation for further measures. Later in 2018, for example, the national police force set up a Cyber Crime Directorate to counter disinformation spread though digital media.[9]

In December 2020 the BSSN released the draft of a new national cyber-security strategy for public consultation.[10] It places greater emphasis on nationally significant cyber incidents and focuses on seven specific areas: risk management in national cyber security; preparedness and resilience; critical information infrastructure; capacity-building; increasing awareness; legislation and regulation; and international cooperation. Other stated objectives include protecting the country from any interference in cyberspace that might disrupt public order, and building on improved cyber security to expand the potential of the digital economy. The new draft follows Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions,[11] which raised the status of the cyber-security strategy by declaring it to be part of national-security policy.

Given the deteriorating security situation in Indonesia, one of the government's priorities has been to counter domestic terrorism and online extremism, as well as to clamp down on political protest. For example, after a large protest in October 2020, disinformation laws were invoked to allow the police to take action online against political activists[12] and Islamist groups, including the Muslim Cyber Army hacker group responsible for spreading religious intolerance online.[13] There is now a debate in Indonesian politics about the extent to which government policy should involve censoring cyberspace.[14]

On military cyber policy, the debates and analyses have generally been more advanced than those in the civil sector but have not always led to concrete progress.

The Ministry of Defence (MoD) laid out comprehensive guidelines for national cyber defence in 2014,[15] with the focus more on securing defence assets against cyber attacks rather than on any concept of sustained cyber-enabled warfare. Besides acknowledging the need for counter-attack capabilities for the purpose of deterrence, the guidelines did not cover offensive cyber.

A 2015 defence white paper went further, presenting cyber defence as one of four pillars of Indonesia's overall defence posture, alongside air defence, strategic strike and electronic warfare.[16] It described cyber security as central to national defence capabilities, highlighted the importance of integrating cyber with all other instruments of national power,[17] and declared a commitment to modernising the country's cyber capabilities.[18]

In 2017 the MoD began promoting a 'civil-defence concept' in coordination with the National Development Planning Agency, aiming to ensure that methods of 'non-military defence' – including in cyberspace – were adopted by all ministries and state institutions.[19] The initiative was widely seen in defence circles as consistent with the country's concept of total defence in which all citizens are regarded as potential combatants, including in cyberspace.

Also in 2017, the armed forces carried out their first major institutional reform by setting up a cyber unit – Satuan Siber, or Satsiber – to develop doctrine, policy, procedures and tactics to deal with cyber threats.[20] Its primary mission is to ensure the cyber security of defence-related critical national infrastructure, though there is a long-term plan to develop offensive capability.[21] Satsiber has also been assigned an early-warning role in monitoring foreign-military movements (especially those of units equipped with missiles) in the immediate region. The development of military cyber strategy and doctrine appears embryonic and there is no substantive evidence of it in unclassified sources.

Governance, command and control

The BSSN, the principal cyber-security agency, operates within the framework of the Coordinating Ministry for Political, Legal and Security Affairs and reports directly to the president.[22] The head of the BSSN has four deputies, responsible for threat identification and detection, protection, response and recovery, and technical policies for monitoring and control.[23] The BSSN set up the first government CERT in 2018,[24] building on the previously existing private CERT and the government's incident-response team.

In the Indonesian armed forces (TNI)[25] there has been clear organisational cyber command and control since the creation of Satsiber in 2017, though the command arrangements are split between the Commander TNI, when Satsiber undertakes military operations,[26] and the Chief of the General Staff, for day-to-day management.

Satsiber has subordinate cyber units in each of the three armed services.[27] Complementing the work of Satsiber, the Cyber Defence Centre[28] operates under the command of the Defence Intelligence Agency within the Ministry of Defence.[29] The technical means for undertaking operational cyber command and control, however, probably mirror the weaknesses in communications systems reported elsewhere in the armed forces.[30]

The Ministry of Foreign Affairs set up its own Digital Command Centre for the twin purposes of improving crisis-management procedures for national emergencies in cyberspace and managing Indonesia's international diplomacy on cyber matters. The combining of two such different functions in one entity is unusual, since crisis management of cyber incidents requires a very different skill set from conducting cyber diplomacy, with little crossover in the day-to-day work of the two missions.

Changes in doctrine, technology and personnel planning are needed if Indonesia is to establish a basic capability for cyber warfare. So too is greater cohesion, as divergent views have been observed among policymakers and those responsible for implementing the development of cyber defence.

Core cyber-intelligence capability

The lead coordinating agency for national civil-sector cyber intelligence is the BSSN.[31] The body mainly responsible for foreign and military intelligence is the Strategic Intelligence Agency (BAIS),[32] which has proved capable of assisting the police by, for example, conducting cyber surveillance against potential threats to the 2018 regional elections.

The BSSN was allocated 2.2 trillion rupiah (US$127 million) in the 2020 budget but its director at the time said 3trn rupiah (US$190m) would be needed to achieve its objectives.[33] The goals he mentioned included developing indigenous technology and the National Cyber Security Operations Centre (tasked with monitoring the digital networks of Indonesia's critical national infrastructure, including the energy, communications and transport systems) and recruiting graduates of the required calibre.[34] This suggests that Indonesia's cyber-intelligence capabilities are relatively unsophisticated and that any wider intelligence reach, beyond the focus on domestic terrorism, is severely under-resourced.

Cyber empowerment and dependence

By 2020 Indonesia had established itself as a rising digital power within the G20, albeit still at a lower level than most other members and with a long way to go to achieve its ambitions in the sector.[35] The government has launched ambitious education programmes, attempted to attract talent through its immigration policies, and promoted a start-up culture.[36] The digital economy was projected to reach double-digit annual growth (11%) in 2020.[37] E-commerce remains the main driver of growth in the economy as a whole. Three of Indonesia's start-ups (Gojek, Tokopedia and Traveloka) have reached high capitalisation levels (US$10.5 billion, US$7.5bn and US$2.75bn respectively), largely by having expanded internationally.[38] The country aspires to become a global hub for Islamic finance, though in that respect it is still in fourth place (behind Malaysia, Saudi Arabia and the United Arab Emirates) in terms of annual value traded.[39]

The average level of digital skills among the Indonesian population does not match the government's ambitions

Although the overall internet penetration rate is quite high (73% of the population in mid-2020),[40] there is a wide gap between Java and all the other islands.[41] There are individual cities with particularly high figures, for example Jakarta (85%), Surabaya (83%) and Bandung (82.5%).[42] More than 90% of Indonesians who use the internet do so via mobile phone. The country was ranked 85th in the 2020 Global Innovation Index, which indicates the weak foundations of its digital economy.[43] The digital sector accounts for only 12% of GDP according to a 2020 estimate,[44] though the government hopes to see that figure rise to 15% by 2025.[45]

The average level of digital skills among the population does not match the government's ambitions.[46] Research commissioned by Amazon Web Services in six Asia-Pacific countries found that only 19% of

Indonesian respondents use digital skills in their jobs – very different from Australia and Singapore, for example, where the corresponding figures are 64% and 63% respectively.[47] The skills shortage could inhibit the development of the indigenous digital industry. Indonesia's reliance on foreign suppliers for its telecommunications infrastructure was highlighted in 2019 during the Huawei controversy, which led a senior official in the Coordinating Ministry for Political, Legal and Security Affairs to declare the need for 'a special, reliable, integrated and secure telecommunications system against cyber threats both from within the country and abroad', and to admit that the existing system had not been able to 'answer the need for national information security'.[48]

Although Indonesia's research in artificial intelligence (AI) is growing, it is still a relative newcomer to the field. It has accelerated efforts to improve collaboration between academia and industry on AI research, for example between the University of Indonesia and Tokopedia[49] and between the Bandung Institute of Technology and Bukalapak.[50] Meanwhile, investment by Indonesian companies in AI solutions is still much lower (US$0.20 per capita) than in more developed economies such as Singapore (US$68 per capita).[51] Nevertheless, it was reported in August 2020 that Indonesia had 74 AI-focused start-ups.[52] Also in August 2020, the government launched a National Strategy for Artificial Intelligence aimed at guiding the development of AI through to 2045.[53] The strategy foreshadows a focus on applying AI to social services, education and research, health services, food security, mobility, smart cities and public-sector reform.[54]

China looks set to make a large contribution to the development of Indonesia's digital economy. Following India's implementation of rules to restrict Chinese takeovers in early 2020, Chinese venture-capital and tech investors have switched their focus to Indonesia, contributing to a 55% surge in investment in the country's tech sector in the first half of 2020.[55] Huawei has forged links with several Indonesian government agencies to help accelerate their digitisation, including through cloud-based infrastructure for storing national data.[56] Besides offering its technology, Huawei has committed to nurture digital talent and boost cyber-security skills in the country.[57] In January 2021, China and Indonesia signed a memorandum of understanding on cooperation and investment in the ICT sector, with a focus on security.[58] While Chinese companies have a large slice of the Indonesian market, they face competition from well-established US, Japanese and European firms. For example, early in 2021, Microsoft announced plans to provide training in digital skills for an additional 3m Indonesians, continuing a commitment in that area that has already lasted for more than 25 years. The initiative is based on a shared project with the Ministry of Communication and Information Technology and four universities, aimed at educating Indonesians in AI, cyber security and data science through a digital-literacy curriculum.[59]

Cyber security and resilience

Indonesian views on cyber security were strongly influenced by the 2013 Edward Snowden leaks about Australia's cyber capabilities, including its monitoring of Indonesia's leaders. Though the country's security agencies were already aware of Australia's espionage activity to some degree, the revelations were a shock to the Indonesian public. The government's response has included the Secretariat General of the National Resilience Council drawing up a national contingency plan against cyber attacks in 2016,[60] and cyber-emergency exercises such as the drill conducted by the national CERT ahead of the 2018 Asian Games in Jakarta.[61] Indonesian specialists have identified high-priority assets that need the strongest protection, including telecommunications and banking networks, online-payment systems and key government, military and private-sector closed networks and data centres.[62] The country's basic cyber defences and incident-response capability are still not highly developed, however.

Indonesia experienced a sixfold increase in cyber attacks between January and October 2020, with its e-commerce firms the major targets. Tokopedia suffered an attack that caused the personal data of 91m users to be leaked, while Bhinneka announced that 1.2m of its accounts had been accessed by hackers.[63] According to a survey by Palo Alto Networks, 84% of Indonesian companies plan to increase their IT budgets, of which

44% intend to allocate more than half of those funds to cyber-security investment.[64]

Apart from launching a public consultation on the new cyber-security strategy in 2020, the government has been pursuing a raft of additional reforms. In February 2021 the BSSN launched a national Computer Security Incident Response Team (CSIRT) that will also serve as the national and the government CSIRT.[65] Fifteen lower-level CSIRTs[66] had already been established in 2020,[67] and the government aims to set up another 27 across its ministries and other public-sector bodies in 2021.[68] In 2020 the BSSN participated in several cyber drills,[69] and in early 2021 it took part in training events on Internet of Things security-testing that were jointly organised with the United States Embassy and Carnegie Mellon University.[70] The BSSN is working with several government agencies in preparing a Draft Presidential Regulation on Vital Information Infrastructure Protection, which will cover the designation of strategic sectors and measures to protect critical information infrastructure, increase cyber readiness and accelerate recovery from cyber incidents.[71] The BSSN has also engaged all relevant owners and operators to ensure their familiarity with the regulations and policies concerning the country's critical information infrastructure.[72]

Despite ambitious policy declarations, Indonesia suffers from a severe shortage of cyber skills. A 2016 study by Oxford University found that the country lacked 'minimal educational programmes in cybersecurity', 'accreditation in cybersecurity education' and a 'national budget to support the cybersecurity capacity programmes'; that there were 'few professional instructors in cybersecurity'; and that knowledge transfer from trained cyber-security employees in the private sector existed only 'on an ad hoc basis'.[73] In 2020, commenting on the national skills shortage, the head of the BSSN reported that typically it took six months for the organisation to fill a cyber-security position.[74] It might therefore take Indonesia two decades or more to develop a sovereign capability for military cyber defence, given the number of sensitive posts requiring cyber expertise that would be needed.

Given that Indonesia is a nation of islands, maritime cyber security is of particular importance. The BSSN has been working on increasing the cyber-security capacity of the Maritime Information Centre.[75] The Indonesian Navy has carried out cyber-defence training since 2016, including a major eight-day exercise in 2018[76] that involved more than 500 personnel and had three main aspects: denial, countermeasures and cyber support for operations.[77] In 2019 the navy added a cyber dimension to its largest annual exercise, *Armada Jaya*.

In the International Telecommunication Union's 2018 Global Cybersecurity Index, Indonesia was ranked 41st out of 175 countries, a low position relative to its wealth and economic ambition.[78]

Global leadership in cyberspace affairs

Since about 2005 the Indonesian government has worked within the frameworks of the Association of Southeast Asian Nations (ASEAN), the ASEAN Regional Forum, the Asia-Pacific Economic Cooperation, the United Nations and the Organisation of Islamic Cooperation (OIC) on various aspects of fighting cyber crime, especially cyber terrorism, and on efforts to build international governance frameworks to promote strategic stability in cyberspace through discussion of cyber norms.

Indonesian specialists who had set up the country's first private CERT worked with Australian and Japanese counterparts to set up the Asia-Pacific CERT (APCERT) in 1998. Indonesia is also a member of the OIC's CERT, of which it became deputy chair in 2018,[79] and has participated in international cyber exercises such as the China–ASEAN Network Security Emergency Response Capacity Building Seminar in 2018.[80] In 2019 Indonesia joined the UN's Group of Governmental Experts[81] on cyber norms, and since 2015 it has staged an annual international cyber conference, CodeBali.[82] In 2020 it participated in the G20 Digital Economy Ministers Meeting that issued a wide-ranging development agenda in the sector, including many security aspects. It has collaborated with China in fighting cyber crime, including by deporting hundreds of Chinese citizens alleged to have been conducting attacks from Indonesia against targets in China.

Offensive cyber capability

Indonesia has reasonably well-developed capabilities for domestic cyber surveillance. For example, a special counter-terrorism unit in the police, Detachment 88, has

been building its cyber-surveillance capabilities with the support of international partners such as Australia.[83]

The available information on any wider offensive cyber capability is patchy, but it suggests Indonesia is weakly positioned to use cyber means to respond during any crisis or period of hostility. The prospect of Indonesia catching up with the offensive cyber capabilities of the states of particular interest to it – such as Australia, China, Malaysia and Vietnam – seems a distant one.

Notes

1 Yudhistira Nugraha, 'The future of cyber security capacity in Indonesia', Oxford Internet Institute, 2016, https://ora.ox.ac.uk/objects/uuid:70392ace-4bd6-4066-818e-a3adc1eeedf3.

2 Its full name is the Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center (ID-SIRTII/CC). See 'History Id-SIRTII/CC', https://idsirtii.or.id/en/page/history-id-sirtii-cc.html.

3 Leonardus K. Nugraha and Dinita A. Putri, 'Mapping the Cyber Policy Landscape: Indonesia', Global Partners Digital, November 2016, pp. 14–15, https://www.gp-digital.org/wp-content/uploads/2017/04/mappingcyberpolicy_landscape_indonesia.pdf.

4 Badan Siber Dan Sandi Negara. See https://bssn.go.id/tentang.

5 More precisely, the BSSN took on the responsibilities of the National Crypto Agency, the Security Incident Response Team on Internet and Infrastructure, and the Information Security Directorate of the Ministry of Communication and Information Technology.

6 Marguerite Afra Sapiie, 'Police Playing Tough in Combating Cybercrimes in Indonesia', *Jakarta Post*, 6 February 2017, https://www.thejakartapost.com/news/2017/02/06/police-playing-tough-in-combating-cybercrimes-in-indonesia-.html.

7 'Kemhan Dorong Pertahanan Nirmiliter Jadi Program Nasional', Antara, 8 May 2019, https://www.antaranews.com/berita/860413/kemhan-dorong-pertahanan-nirmiliter-jadi-program-nasional.

8 Badan Siber Dan Sandi Negara, 'Indonesian Cyber Security Strategy', https://bssn.go.id/strategi-keamanan-siber-nasional.

9 Cabinet Secretariat of the Republic of Indonesia, 'Cyber Crime Directorate Established to Combat Fake News', 4 October 2018, https://setkab.go.id/en/cyber-crime-directorate-established-to-combat-fake-news.

10 Badan Siber Dan Sandi Negara, 'Strategi Keamanan Siber Nasional', 14 December 2020, https://cloud.bssn.go.id/s/qQZmyWaFf8ooc26/download.

11 Karis Kuniaran, 'Ini Strategi BSSN Perkuat Keamanan Siber Nasional', Merdeka, 14 December 2020, https://www.merdeka.com/peristiwa/ini-strategi-bssn-perkuat-keamanan-siber-nasional.html.

12 Usman Hamid and Ary Hermawan, 'Indonesia's Shrinking Civic Space for Protests and Digital Activism', Carnegie Endowment for International Peace, 17 November 2020, https://carnegieendowment.org/2020/11/17/indonesia-s-shrinking-civic-space-for-protests-and-digital-activism-pub-83250.

13 Thomas Paterson, 'Indonesian cyberspace expansion: A double-edged sword', *Journal of Cyber Policy*, vol. 4, no. 2, 2019, pp. 216–34, https://www.tandfonline.com/doi/pdf/10.1080/23738871.2019.1627476?needAccess=true.

14 *Ibid*., p. 217.

15 Peraturan Menteri Pertahanan Republik Indonesia, Nomor 82 tahun 2014 tentang, Pedoman Pertahanan Siber, https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf.

16 Defence Ministry of the Republic of Indonesia, 'Defence White Paper 2015', November 2015, p. 109, https://www.kemhan.go.id/wp-content/uploads/2016/05/2015-INDONESIA-DEFENCE-WHITE-PAPER-ENGLISH-VERSION.pdf.

17 *Ibid*., p. 110.

18 *Ibid*., p. 45.

19 'Kemhan Dorong Pertahanan Nirmiliter Jadi Program Nasional', Antara.

20 Satsiber, 'Sejarah', https://satsiber-tni.mil.id/sejarah-20181230304.

21 Sri Hidayati and Rudi A.G. Gultom, 'Analisis Kebutuhan Senjata Siber Dalam Meningkatan Pertahanan Indonesia Di Era Peperangan Siber', *Teknologi Persenjataan*, vol. 1, no. 1, 2020, p. 90, http://139.255.245.7/index.php/TPJ/article/viewFile/474/451.

22 'Jokowi Strengthens Role of Cyber Agency', *Tempo*, 3 January 2018, https://en.tempo.co/read/914520/jokowi-strengthens-role-of-cyber-agency.

23 Badan Siber Dan Sandi Negara, 'Pimpinan Badan Siber Dan Sandi Negara', https://bssn.go.id/pejabat.

24 Mehda Basu and Yun Xuan Poon, 'Five steps in Indonesia's cyber battle plan: Interview with Lieutenant General (ret) Hinsa Siburian, Head of the National Cyber and Encryption Agency (BSSN),

Indonesia', GovInsider, 17 September 2020, https://govinsider.asia/security/bssn-five-steps-in-indonesias-cyber-battle-plan.

25 Tentara Nasional Indonesia

26 TNI, 'Organizational Structure', https://int.tni.mil.id/struktur.html. See also Sekretariat Kabinet Republik Indonesia, 'Inilah Perpres No. 62 Tahun 2016 Tentang Susunan Organisasi Tentara Nasional Indonesia (1)', 19 January 2017, https://setkab.go.id/inilah-perpres-no-62-tahun-2016-tentang-susunan-organisasi-tentara-nasional-indonesia-1.

27 The Satsiber unit within the Indonesian Air Force was formally inaugurated only in September 2020. See Achmad Nasrudin Yahya, 'Bentuk Peperangan Makin Tak Dapat Diprediksi, TNI AU Bentuk Satuan Siber', *Kompas*, 17 September 2020, https://nasional.kompas.com/read/2020/09/17/07393261/bentuk-peperangan-makin-tak-dapat-diprediksi-tni-au-bentuk-satuan-siber.

28 Pushansiber. See Kementerian Pertahanan Republik Indonesia, 'Kapushansiber', https://www.kemhan.go.id/bainstrahan/kapushansiber.

29 See Kementerian Pertahanan Republik Indonesia, 'Badan Instalasi Strategis Pertahanan', https://www.kemhan.go.id/bainstrahan.

30 Alex Firmansiyah Rahman, Syaiful Anwar and Arwin Datumaya Wahyudi Sumari, 'Analisis Minimum Essential Force (MEF) Dalam Rangka Pembangunan Cyber-Defense', *Jurnal Pertahanan & Bela Negara*, vol. 5, no. 3, 2018, pp. 63–85, http://jurnal.idu.ac.id/index.php/JPBH/article/view/370.

31 Margareth S. Aritonang, 'Police to Support National Cyber Agency', *Jakarta Post*, 4 January 2017, https://www.thejakartapost.com/news/2017/01/04/police-to-support-national-cyber-agency.html.

32 Badan Intelijen Strategis

33 'DPR "Ngotot" Perjuangkan Dana Rp20 Triliun Untuk BSSN', CNN Indonesia, 13 November 2019, https://www.cnnindonesia.com/teknologi/20191113191757-185-448102/dpr-ngotot-perjuangkan-dana-rp20-triliun-untuk-bssn.

34 *Ibid*.

35 European Center for Digital Competitiveness, 'Digital Riser Report 2020', September 2020, https://digital-competitiveness.eu/wp-content/uploads/ESCP_Digital-Riser-Report_2020-1.pdf.

36 *Ibid*., p. 7.

37 'e-Conomy SEA 2020 – At full velocity: Resilient and racing ahead', Google, Temasek, Bain & Company, November 2020, p. 32, https://www.thinkwithgoogle.com/_qs/documents/10614/e-Conomy_SEA_2020_At_full_velocity__Resilient_and_racing_ahead_bMmKO5b.pdf.

38 For Gojek and Tokopedia valuations, see 'Indonesia's Gojek Mulls $18 Billion Merger With Tokopedia', PYMTS.com, 5 January 2021, https://www.pymnts.com/news/partnerships-acquisitions/2021/indonesias-gojek-mulls-18-billion-merger-with-tokopedia. For a Traveloka valuation, see Yoolim Lee, 'Traveloka Nears Fundraising at Lower Valuation', Bloomberg Quint, 10 July 2020, https://www.bloombergquint.com/business/traveloka-is-said-near-fundraising-at-sharply-lower-valuation.

39 Fauziah Rizki Yuniarti, 'Indonesia could be Asia's next Islamic finance hub', *Jakarta Post*, 12 January 2021, https://www.thejakartapost.com/academia/2021/01/12/indonesia-could-be-asias-next-islamic-finance-hub.html.

40 Eisya A. Eloksari, 'Indonesian internet users hit 196 million, still concentrated in Java: APJII survey', *Jakarta Post*, 11 November 2020, https://www.thejakartapost.com/news/2020/11/11/indonesian-internet-users-hit-196-million-still-concentrated-in-java-apjii-survey.html.

41 *Ibid*.

42 'Indonesian Internet Users Reach 200 Million Until 2Q of 2020', The Insider Stories, 10 November 2020, https://theinsiderstories.com/indonesian-internet-users-reach-200-million-until-2q-of-2020.

43 'Global Innovation Index 2020: Who Will Finance Innovation?', SC Johnson College of Business – Cornell University, INSEAD and WIPO, September 2020, p. 17, https://www.globalinnovationindex.org/Home.

44 Vience Mutiara Rumata and Ashwin Sasongko Sastrosubroto, 'The Paradox of Indonesian Digital Economy Development', IntechOpen, 27 May 2020, https://www.intechopen.com/online-first/the-paradox-of-indonesian-digital-economy-development.

45 'Incar Jawara Dunia, Inilah Strategi RI Dalam Ekonomi Digital', Kementerian Komunikasi dan Informatika Republik Indonesia, November 2018, http:///content/detail/15306/incar-jawara-dunia-inilah-strategi-ri-dalam-ekonomi-digital/0/sorotan_media.

46 Trisha Ray et al., 'The Digital Indo-Pacific: Regional Connectivity and Resilience', Quad Tech Network, ANU, CNAS, GRIPS, ORF, February 2021, p. 17, https://crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2021-02/thedigitalindopacific.pdf.

47 Eileen Yu, 'Cloud, Data amongst APAC Digital Skills Most Needed', ZDNet, 25 February 2021, https://www.zdnet.com/article/cloud-data-amongst-apac-digital-skills-most-needed/.

48 Coordinating Ministry for Political, Legal and Security Affairs, 'Tingkatkan Keamanan Informasi Nasional, Deputi VII Kominfotur Laksanakan FGD Merevival Kedaulatan Telekomunikasi', 27 June 2019, https://polkam.go.id/tingkatkan-keamanan-informasi-nasional-deputi-vii-kominfotur-laksanakan.

49 'UI Gandeng Tokopedia Bangun Pusat Penelitian Kecerdasan Buatan, Menristekdikti Harapkan Lulusan Indonesia Penuhi Kebutuhan SDM Perusahaan Startup', Ristek-Brin, 28 March 2019, https://www.ristekbrin.go.id/ui-gandeng-tokopedia-bangun-pusat-penelitian-kecerdasan-buatan-menristekdikti-harapkan-lulusan-indonesia-penuhi-kebutuhan-sdm-perusahaan-startup.

50 Arya Dipa, 'Bukalapak, ITB Launch AI, Cloud Computing Innovation Center', *Jakarta Post*, 2 February 2019, https://www.thejakartapost.com/news/2019/02/02/bukalapak-itb-launch-ai-cloud-computing-innovation-center.html.

51 Dylan Loh, 'ASEAN Faces Wide AI Gap as Vietnam and Philippines Lag Behind', *Nikkei Asia*, 9 October 2020, https://asia.nikkei.com/Business/Technology/ASEAN-faces-wide-AI-gap-as-Vietnam-and-Philippines-lag-behind2.

52 Hugh Harsono, 'Why Indonesia Is Poised to Become the Next AI Start-up Hub', *South China Morning Post*, 25 August 2020, https://www.scmp.com/tech/article/3098596/why-indonesia-poised-become-next-ai-start-hub.

53 Indonesia National Secretariat of Artificial Intelligence, 'Indonesia National Strategy for Artificial Intelligence', 10 August 2020, https://ai-innovation.id/strategi.

54 *Ibid*.

55 Mercedes Ruehl, 'China's Tech Investors Turn from India to Indonesia', *Financial Times*, 29 November 2020, https://www.ft.com/content/bcc935fd-ef40-4d6d-9939-ea18498e0283.

56 'Cybersecurity Becomes BSSN's Challenge in the Digitalization of Indonesia', Waktunya Merevolusi Pemberitaan, 28 August 2020, https://voi.id/en/technology/12457/cybersecurity-becomes-bssns-challenge-in-the-digitalization-of-indonesia.

57 The Huawei ASEAN Academy reportedly comprises business, technical and engineering colleges with 100 trainers, more than 3,000 courses and more than 100 mirroring environments.

58 Chris Devonshire-Ellis, 'Investment Infrastructure Projects in Indonesia Contributing to Improved Manufacturing Capability', ASEAN Briefing, 4 February 2021, https://www.aseanbriefing.com/news/investment-infrastructure-projects-in-indonesia-contributing-to-improved-manufacturing-capability.

59 'Microsoft to Establish First Datacenter Region in Indonesia as Part of Berdayakan Ekonomi Digital Indonesia Initiative', Microsoft Stories Asia, 25 February 2021, https://news.microsoft.com/apac/2021/02/25/microsoft-to-establish-first-datacenter-region-in-indonesia-as-part-of-berdayakan-digital-economy-indonesia-initiative/.

60 Arif Rahman and Oktarina Paramitha Sandy, 'Ini Urgensi UU Keamanan dan Ketahanan Siber' [interview with Colonel Arwin Datumaya Wahyudi Sumari], Cyberthreat.id, 26 April 2019, https://cyberthreat.id/read/305/Ini-Urgensi-UU-Keamanan-dan-Ketahanan-Siber.

61 Asia Pacific Computer Emergency Response Team, 'APCERT Annual Report 2018', p. 125, http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2018.pdf.

62 Achmad Rouzni Noor, 'Strategi Indonesia Menjaga Kedaulatan Cyber', detikinet, 1 February 2016, https://inet.detik.com/cyberlife/d-3131768/strategi-indonesia-menjaga-kedaulatan-cyber.

63 'Covid-19 and Cyberattacks: Which Emerging Markets and Sectors Are Most at Risk?', Oxford Business Group, 17 February 2021, https://oxfordbusinessgroup.com/news/covid-19-and-cyberattacks-which-emerging-markets-and-sectors-are-most-risk.

64 Eisya A. Eloksari, 'Indonesian Businesses Ramp up Cybersecurity Budget amid Rampant Attacks', *Jakarta Post*, 23 July 2020, https://www.thejakartapost.com/news/2020/07/22/indonesian-businesses-ramp-up-cybersecurity-budget-amid-rampant-attacks.html.

65 'Kepala BSSN Resmikan Tim Tanggap Insiden Keamanan Siber (BSSN-CSIRT) Demi Tercipta Ruang Siber Yang Aman Dan Kondusif', Badan Siber Dan Sandi Negara, 25 February 2021, https://bssn.go.id/kepala-bssn-resmikan-tim-tanggap-insiden-keamanan-siber-bssn-csirt-demi-tercipta-ruang-siber-yang-aman-dan-kondusif/.

66 In 2020 the BSSN established CSIRTs in institutions including the Ministry of Finance and the Ministry of Education and Culture, and in provinces including Central Java, East Java, Gorontalo, Jakarta, the Riau Islands, West Java and West Sumatra. See 'BSSN Gandeng Pemprov DKI Jakarta Bentuk Tim Tanggap Insiden Keamanan Siber', Badan Siber Dan Sandi Negara, 23 December 2020, https://bssn.go.id/bssn-gandeng-pemprov-dki-jakarta-bentuk-tim-tanggap-insiden-keamanan-siber; and 'Resmikan Jogjaprov CSIRT, BSSN Harap Bisa Tekan Ancaman Siber di Yogyakarta', KOMPAS.com, 15 October 2020, https://biz.kompas.com/read/2020/10/15/133036728/resmikan-jogjaprov-csirt-bssn-harap-bisa-tekan-ancaman-siber-di-yogyakarta.

67 'Resmi Dibentuk, Kemenkeu-CSIRT Menutup Program Prioritas Strategis BSSN Di Tahun 2020', Badan Siber Dan Sandi Negara, 29 December 2020, https://bssn.go.id/resmi-dibentuk-kemenkeu-csirt-menutup-program-prioritas-strategis-bssn-di-tahun-2020.

68 *Ibid.*

69 These drills include the ITU Cyber Drill Exercise 2020, ASEAN Cert Incident Drill 2020, OIC Cert Cyber Drill 2020, Critical Information Infrastructure Cyber Exercise 2020, ASEAN Japan Cyber Exercise 2020 and APCERT Drill 2020. See Id-SIRTII/CC, 'Activity', 2020, https://idsirtii.or.id/en/activity/year/2020.html.

70 'APCERT Training: Implementing IoT Security Testing', ID-SIRTII/CC, 23 February 2021, https://idsirtii.or.id/en/activity/detail_year/2021/92/apcert-training-implementing-iot-security-testing.html; and 'Carnegie Mellon University: Unhide Hidden Cobra', ID-SIRTII/CC, 15 February 2021, https://idsirtii.or.id/en/activity/detail_year/2021/94/carnegie-mellon-university-unhide-hidden-cobra.html.

71 'BSSN Beserta 13 Lembaga Pemerintah Formulasikan Rancangan Perpres Perlindungan Infrastruktur Informasi Vital', Badan Siber Dan Sandi Negara, 10 February 2021, https://bssn.go.id/bssn-beserta-13-lembaga-pemerintah-formulasikan-rancangan-perpres-perlindungan-infrastruktur-informasi-vital.

72 'BSSN Gelar Diseminasi Peraturan dan Kebijakan Sektor Infrastruktur Informasi Kritikal Nasional (IIKN)', Badan Siber Dan Sandi Negara, 10 February 2021, https://bssn.go.id/bssn-gelar-diseminasi-peraturan-dan-kebijakan-sektor-infrastruktur-informasi-kritikal-nasional-iikn.

73 Nugraha, 'The future of cyber security capacity in Indonesia', pp. 12, 55.

74 Basu and Yun, 'Five steps in Indonesia's cyber battle plan: Interview with Lieutenant General (ret) Hinsa Siburian, Head of the National Cyber and Encryption Agency (BSSN), Indonesia'.

75 'BSSN Menerima Kunjungan Bakamla Dalam Rangka Kerjasama Keamanan Informasi', Badan Siber Dan Sandi Negara, 4 February 2021, https://bssn.go.id/bssn-menerima-kunjungan-bakamla-dalam-rangka-kerjasama-keamanan-informasi.

76 TNI, 'TNI AL Tingkatkan Kemampuan Pertahanan Siber', 6 November 2018, https://tni.mil.id/view-140439-tni-al-tingkatkan-kemampuan-pertahanan-siber.html.

77 Satsiber, 'Gubernor Aaal Hadiri Latihan Operasi Pertahanan Siber TNI AL 2018', 12 December 2018, https://satsiber-tni.mil.id/gubernur-aal-hadiri-latihan-operasi-pertahanan-siber-tni-al-2018-20181212674.

78 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 58, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

79 Asia Pacific Computer Emergency Response Team, 'APCERT Annual Report 2018', p. 128.

80 *Ibid.*, p. 88.

81 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.

82 See 'CodeBali International Cyber Security Conference and Exhibitions' website, https://codebali.id.

83 Muhammad Nadjib and Hafied Cangara, 'Cyber Terrorism Handling in Indonesia', *Business and Management Review*, vol. 9, no. 2, November 2017, pp. 278–9, https://cberuk.com/cdn/conference_proceedings/conference_30092.pdf.

14. Malaysia

On cyber security, Malaysia was a regional first mover and compares well with many other countries. Its ongoing commitment was demonstrated in 2020 with new cyber-security strategies for the civil sector and for national defence. There is little information available on core cyber-intelligence capabilities or the development of offensive cyber, with the policy statements issued in 2020 focusing more on active defence in cyberspace. Malaysia has prioritised the development of an indigenous digital-industrial base in support of its wider economic-development agenda. It compensates for some of its shortcomings in cyber capability through international alliances, particularly with the United States, the United Kingdom, Australia and Singapore. Overall, Malaysia is a third-tier cyber power but has clear strengths in cyber-security policy and strong digital-economic potential. If it realises that potential, it could create the foundations on which to become a second-tier cyber power.

Strategy and doctrine

The development of Malaysia's cyber policies, strategy and doctrine has been shaped more by its industrialisation and development agenda than by international-security considerations. Closely tied to the economic imperative is the aim of guaranteeing a free and open digital environment for innovation and the need for a stable domestic environment to underpin investment. The country's cyber policies have also been shaped by the high priority successive governments have attached to issues of internal security.

Malaysia's interest in cyberspace can be traced back to the 1990s, when the government first recognised the potential of the internet to transform its provision of public services and catalyse the country's development. It set out to foster a digital ecosystem through a combination of public policies and incentives for businesses, including significant investment in creating the necessary technical infrastructure. The goal was to accelerate the transition from an agriculture-based economy to one based on manufacturing and services, and then ultimately to a fully fledged knowledge economy.

In 2006 the government announced a National Cyber Security Policy (NCSP) that identified 'ten pillars' of 'Critical National Information Infrastructure' and recognised their interdependence.[1] The NCSP outlined a piecemeal approach to building up cyber-security capabilities at the national level.

In 2016 the government published a Public Sector Cyber Security Framework to consolidate the various directives since 2000 that had been aimed at bolstering

List of acronyms

ASEAN	Association of Southeast Asian Nations
CDOC	Cyber Defence Operations Centre
CERT	Computer Emergency Response Team
ICT	information and communications technology
IoT	Internet of Things
MAF	Malaysian Armed Forces
MoD	Ministry of Defence
NACSA	National Cyber Security Agency
NSC	National Security Council

public-sector cyber resilience,[2] and in 2017 the Ministry of Defence (MoD) introduced an ICT security policy that included an ICT steering committee responsible for assessing and approving ICT needs within the MoD and the Malaysian Armed Forces (MAF). The committee is chaired by the MoD's secretary-general or their deputy. There is also a technical committee to oversee technical aspects of the MoD's and the MAF's ICT requirements.[3]

A new Cyber Security Strategy, covering the period 2020–24, was released in 2020.[4] It was the first such document since 2006, and addressed five pillars of policy: governance, legislative framework and enforcement, world-class innovation, capacity-building and education, and global collaboration. It covered much of the same ground as the corresponding strategies in other states, particularly in its emphasis on fighting cyber crime, protecting critical national infrastructure, innovation, and educating more people to fill gaps in the cyber workforce. Its other priorities included fighting terrorism and violent extremism, especially by countering internet-based incitement and recruitment. It stated a commitment to pursuing three broad strategic priorities: the governance ecosystem, improving private-sector security (especially for infrastructure operators) and improving the handling of cyber-security incidents. The government announced that the strategy would entail investment of US$434 million over the four-year period.[5]

A 2020 defence white paper announced a much stronger policy direction towards active cyber defence across the civil and military sectors.[6] It also implied the development of some offensive cyber capability, albeit to be used only in response to a cyber attack on Malaysia. It identified three pillars of national-defence strategy – concentric deterrence, comprehensive defence and credible partnerships – and emphasised cyber resilience as part of a whole-of-society concept of defence.

The white paper presented the concept of the 'Future Force' that would be needed to implement concentric deterrence. One of its central characteristics would be 'interoperability', indicating a commonality of doctrines, procedures, systems and equipment across the MAF. The Future Force would also be 'technology-based', meaning it would incorporate the latest digital technologies by, for example, embracing the Internet of Things (IoT) and artificial intelligence (AI). The white paper tasked the MAF with reviewing existing doctrine in order to incorporate more automated and autonomous technologies, including reforming the force structure and posture where necessary.[7]

In many ways the aspirations presented in the 2020 defence white paper were similar to those in a much earlier document, the National Defence Policy of 2010, which had emphasised the importance of information-domain dominance at the operational, tactical and strategic levels in order to protect national sovereignty.[8] It had stated that developing a cyber-warfare capability would be an 'important step towards counterbalancing the ability of other countries in the region and to defend important national targets from all forms of threats'.

Governance, command and control

The National Security Council (NSC), chaired by the prime minister, is the highest decision-making body on cyber-security matters. It has a sub-committee on cyber security, chaired by a senior security minister, which met for the first time in December 2020.[9] The sub-committee is supported by the National Cyber Security Agency (NACSA), created in 2017, which takes the lead at the national level in formulating, overseeing, coordinating and synchronising the implementation of cyber-security policy across the public and private sectors. NACSA's responsibilities also include legislative and enforcement efforts related to cyber security and internal and external collaboration covering both the public and private sectors.[10] NACSA coordinates all the other government agencies that intersect with cyber security, including the Attorney General's Chambers, the office of the Chief Government Security Officer, CyberSecurity Malaysia, the Ministry of Communications and Multimedia, and the Ministry of Domestic Trade and Consumer Affairs.[11]

In 2016 the MoD and the MAF established a Cyber Defence Operations Centre (CDOC) to protect their collective ICT systems and networks. Fully operational since 2017, the CDOC monitors threats and mitigates the impacts of cyber-security incidents.[12] In December 2020, after more than a year of planning, the MAF announced the creation of the Defence Communication and Electronic Division tasked with

improving offensive and defensive capabilities for cyber operations, and conducting electronic warfare.[13] This replaced the Communications and Electronics Division, created in 1993.

Both the MoD and the MAF have their own Computer Emergency Response Teams (CERTs) – MinDefCERT and MAFCERT respectively. MinDefCERT reports incidents to the government CERT (GCERT MAMPU) whereas MAFCERT reports directly to the NSC. MAFCERT is led by the head of the CDOC and includes the ICT managers working in each of the three armed services.[14]

Core cyber-intelligence capability

Malaysia's intelligence community is directed by the NSC under the Prime Minister's Department,[15] whose main role is to coordinate national-security policies, including during emergencies.[16] Among its ten subdivisions are the National Intelligence Committee (NIC) and its supporting National Intelligence Division.[17] The NIC is tasked with coordinating the work of the other intelligence agencies, namely Special Branch (under the Royal Malaysia Police), the Malaysian External Intelligence Organisation (under the Prime Minister's Department) and the Defence Staff Intelligence Division (under the MAF).

The main signals-intelligence capability lies with the Royal Signals Regiment (RSD)[18] and the Royal Intelligence Corps, in the army, and the Defence Staff Intelligence Division (equivalent to the US Defense Intelligence Agency), as part of a very broad suite of national-security missions and tasks. MAF restructured the RSD in 2018, which resulted in the creation of a specialised cyber unit (designated 99 RSD).[19] Special Branch conducts cyber surveillance of internal threats from terrorism and subversion. The Malaysian foreign-intelligence organisation, formally known as the Research Department of the Prime Minister, may have a small cyber-intelligence unit.

Malaysia relies on collaboration with international partners, especially the United States, the United Kingdom, Australia and Singapore, for the wider regional and global cyber-intelligence picture. Security cooperation between Kuala Lumpur and these other countries is tied closely to intelligence collection in the South China Sea and to counter-terrorism.

Cyber empowerment and dependence

Malaysia's digital economy contributes about 20% of GDP[20] and the government anticipates that through technological innovation the sector can play an increasing role in economic growth.[21] Leading this effort is the Malaysia Digital Economy Corporation,[22] whose role includes overseeing the development of the Multimedia Super Corridor (modelled on California's Silicon Valley), home to almost 3,000 ICT companies.[23] In partnership with the private sector the government has launched numerous policies and road maps related to the digital economy, including the National Industry 4WRD Policy, focused on Industry 4.0; the National eCommerce Roadmap; a national Big Data Analytics ecosystem; a Digital Free Trade Zone, aimed at making Malaysia an e-commerce and e-fulfilment hub; and a National IoT Framework.[24] A National AI Framework is also being drafted.

In 2019 the Ministry of Communications and Multimedia recorded 43.38m broadband subscriptions among Malaysia's population of 32m.[25] However, there is an urban–rural digital divide, with at least 3.5m Malaysians in rural or semi-urban areas having very slow internet speeds.[26] The National Fiberisation and Connectivity Plan aims to establish a fibre network serving 70% of schools, hospitals, libraries, police stations and post offices by 2022, and to provide average internet speeds of 30 Mbps in 98% of populated areas by 2023.[27]

Malaysia's AI research capabilities are less developed than those of some other Southeast Asian states

Malaysia's AI research capabilities are less developed than those of some other Southeast Asian states. For example, in a ranking of the world's top 50 countries based on their contributions to the two most prestigious AI conferences in 2020, Malaysia was placed 47th, which was lower than Singapore (12th), Vietnam (27th) and Thailand (44th) but ahead of Indonesia, which did not feature in the list.[28] There have been some notable investments in AI in the private sector. In 2020, G3 Global Bhd, a Malaysian company specialising in IoT solutions and

AI, signed an agreement with two Chinese tech companies to establish Malaysia's first AI park in Kuala Lumpur, apparently aiming to invest more than US$1 billion by 2025.[29] Malaysia's AI-adoption rate (8.1%) is still slow compared with, for example, Indonesia (24.6%) or Thailand (17.1%).[30]

Most of the country's fibre-optic cables are owned and operated by two corporations, either directly or through shareholdings in smaller companies. Tenaga Nasional Berhad, Malaysia's largest electricity company,[31] owns 12,000 kilometres of fibre-optic cables nationwide, using only a small portion of the available bandwidth.[32] Telekom Malaysia Berhad, which has links to the government and is the only company with a high-speed broadband network as part of a public–private partnership, wires 2.5m homes across the country. Worldwide, it has more than 20 undersea cable systems, spanning more than 190,000 km, and more than 560,000 km of fibre-optic cables.[33] Malaysia itself is served by only four undersea cables. The other, smaller companies that run their own fibre-optic cables are Fibrecomm, with 110,000 km of cables nationwide;[34] TIME dotCom, with 7,000 km running throughout the North–South Expressway; and Fiberail, with 4,800 km along railway tracks. Mobile-telecommunications companies such as Celcom Axiata, Digi and Maxis also own fibre networks.[35] In December 2020, Penang became the first Malaysian state to make fibre-optic cabling mandatory in new property developments.[36]

Malaysia's satellite-communications capability is operated by MEASAT Global Berhad, which has a fleet of five satellites with coverage over Asia, the Middle East and Africa. It has commissioned Airbus to build a new satellite, MEASAT-3d, to be launched in 2021. This would enhance the delivery of 4G and 5G mobile networks.[37]

Cyber security and resilience

Malaysia was a regional first mover in cyber-security policy. With its Computer Crime Act of 1997, it was one of the first countries in Asia to enact legislation related to computer offences.[38] In 2008 it was accorded the unique honour of becoming the repository of the Global Cybersecurity Agenda (GCA) launched by the International Telecommunication Union (ITU).[39] A supervisory and regulatory authority, the Communications and Multimedia Commission, had been in place since 1998,[40] and a Personal Data Protection Act was passed in 2010.[41]

In 2011 Malaysia created a National Cyber Coordination and Command Centre to monitor and manage cyber incidents, and to determine the level and potential impact of cyber-security threats.[42] It receives data from CyberSecurity Malaysia and the Malaysian Communications and Multimedia Commission,[43] whose mission during a crisis is to perform a technical advisory role in support of the National Cyber Crisis Management Committee.[44]

Malaysia has the potential to achieve an advanced level of cyber resilience

A pilot project to tackle malware threats at the national level has been implemented under the Coordinated Malware Eradication and Remediation Project, and the ITU's 2018 Global Cybersecurity Index highlights several inter-agency initiatives to combat online banking fraud, operate digital forensic laboratories and exchange information in technical areas of cyber security. There is also collaboration between the government and industry to develop best-practice guidelines for cloud security.[45]

Malaysian and multinational companies play important roles in increasing the country's resilience against cyber threats, working with the government to boost domestic capacity and capability. The Malaysian company Cyber Intelligence, for example, has set up cyber ranges in collaboration with CyberSecurity Malaysia and the International Islamic University Malaysia.[46]

At the technical level, Malaysia began conducting national cyber drills involving public and private stakeholders in the Critical National Information Infrastructure in 2008. Codenamed X-Maya and led by CyberSecurity Malaysia and the National Security Council, those drills tested the technical and collaborative skills of personnel throughout each 'pillar' of the infrastructure.[47] The latest public reporting of such drills was in 2017. Since then, government policy

seems to have focused on a sector-based approach, for example requiring financial institutions to develop cyber-incident-response plans and to test them by holding annual exercises.[48] The 2020 Cyber Security Strategy prioritised the enhancement of measures to protect critical national infrastructure, including much stronger obligations for the operators of that infrastructure to prevent cyber incidents or, if they occur, to mitigate their consequences.[49]

Given that the key cyber-security foundations are in place – especially policy commitment on the part of the government, and high-quality education in the field – Malaysia has the potential to achieve an advanced level of cyber resilience. It was ranked eighth out of 175 countries in the ITU's 2018 Global Cybersecurity Index, and second in the Asia-Pacific region behind Singapore.[50] But questions remain about the detection and reporting of cyber attacks, and about incident-response capabilities. There appears to be room for improvement when it comes to coordination between cyber-security actors, with one 2019 analysis reporting a 'lack of unity of effort'.[51]

Global leadership in cyberspace affairs

On the technical front, Malaysia continues to play a leading role in regional and global forums. Through CyberSecurity Malaysia the country has become the permanent secretariat of the Organisation of Islamic Cooperation's Computer Emergency Response Team (OIC-CERT). It conducted the first Association of Southeast Asian Nations (ASEAN) cyber capacity-building programme in 2015, and has served twice as deputy chair of the Asia-Pacific CERT (APCERT). CyberSecurity Malaysia's digital forensic laboratory – which can conduct computer, multimedia, mobile, biometric, cloud-computing and embedded-device forensics – was the first in the Asia-Pacific to receive Interpol recognition.[52]

Malaysia has also contributed to various other technical and standards-related platforms, including the Forum of Incident Response and Security Teams, the Internet Corporation for Assigned Names and Numbers, the ASEAN Telecommunications and Information Technology Ministers' Meeting, and the Asia-Pacific Telecommunity.[53]

On the international-security front, Malaysia has been actively leading discussions within the ASEAN Regional Forum (ARF) for several years. It co-chairs, together with Japan and Singapore, the ARF Inter-Sessional Meeting on the Security and Use of Information and Communications Technology, whose objectives include assessing 'regional needs for capacity building on ICTs Security' and assisting 'the development of a peaceful, secure, open and cooperative environment for the expansion of ICTs Security among ARF Participants'.[54]

Malaysia also participated in the United Nations Group of Governmental Experts (GGE)[55] in 2014–15, which produced a consensus report on possible voluntary norms despite the widely differing views and interests of its members,[56] and in regional capacity-building efforts to promote, clarify and initiate implementation of the GGE's 11 norms within Southeast Asia.[57]

Offensive cyber capability

Aside from the aspirations set out in the 2010 National Defence Policy and the 2020 defence white paper, there has been little indication of Malaysian activity in the sphere of offensive cyber. Policy guidance at the highest levels suggests that the government's overriding priority is to use cyberspace to further its economic-development agenda, and this priority is not expected to shift. Any progress towards achieving offensive cyber ambitions is therefore likely to remain slow.

Notes

1 Ministry of Science, Technology and Innovation, Malaysia, 'National Cyber Security Policy: The Way Forward', Federal Government Administrative Centre, July 2006, https://cnii.cybersecurity.my/main/ncsp/tncsp.html. The ten pillars of

Critical National Information Infrastructure outlined in the policy were national defence and security; banking and finance; information and communications; energy; transportation; water; health services; government; emergency services; and food and agriculture.

2 See National Cyber Security Agency, 'RAKKSSA: Rangka Kerja Keselamatan Siber Sektor Awam', April 2016, https://www.nacsa.gov.my/doc/RAKKSSA-VERSI-1-APRIL-2016-BM.pdf.

3 See 'Dasar Keselamatan Teknologi Maklumat Dan Komunikasi (DKICT)', January 2017, http://www.stride.gov.my/v2/images/contents/DKICT-MINDEF_VER-5_1-JAN-2017.pdf.

4 National Security Council, Prime Minister's Department, 'Malaysia Cyber Security Strategy 2020–2024', October 2020, https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf.

5 Stuart Crowley, 'Malaysia to spend $434m on national cybersecurity strategy', W.media, 16 October 2020, https://w.media/malaysia-to-spend-434m-on-national-cybersecurity-strategy/#:~:text=The%20first%20pillar%20will%20look,and%20formulating%20laws%20on%20cybersecurity.

6 Ministry of Defence, 'Defence White Paper: A Secure, Sovereign and Prosperous Malaysia', Kuala Lumpur, 2020, http://www.mod.gov.my/images/mindef/article/kpp/DWP.pdf.

7 *Ibid*.

8 'Malaysia's National Defence Policy', 2010, pp. 12–13, https://web.archive.org/web/20181024164353/http://www.mod.gov.my/images/mindef/lain-lain/ndp.pdf.

9 'National Security Council: Govt to set up special task force to identify cyber security issues', *Malay Mail*, 17 December 2020, https://www.malaymail.com/news/malaysia/2020/12/17/national-security-council-govt-to-set-up-special-task-force-to-identify-cyb/1932893.

10 National Security Council, Prime Minister's Department, 'Frequently Asked Questions', https://www.nacsa.gov.my/faq.php.

11 *Cyber Security – Towards a Safe and Secure Cyber Environment* (Kuala Lumpur: Academy of Sciences Malaysia, 2018), pp. 30–3, https://issuu.com/asmpub/docs/cybersecurity.

12 Muhammad Sabu, *Hansard,* Parliament of Malaysia, D.R.30.10.2018, 30 October 2018, p. 137.

13 'Launch Ceremony of Cyberand Electromagnetic Division Defence (BSEP)', *Malaysia Military Times*, 19 December 2020, https://mymilitarytimes.com/index.php/2020/12/19/launch-ceremony-of-cyber-and-electromagnetic-division-defence-bsep. Note that there are different English translations of the entity's name. The name used by the MAF is the Defence Communication and Electronic Division.

14 'Dasar Keselamatan Teknologi Maklumat Dan Komunikasi (DKICT)', pp. 23–5.

15 National Security Council, 'Directive No. 20, Policy and Mechanism of National Disaster Management and Relief', https://www.adrc.asia/management/MYS/Directives_National_Security_Council.html.

16 Majlis Keselamatan Negara, 'Sejarah', 20 January 2019, https://www.mkn.gov.my/web/ms/sejarah-mkn.

17 Philip H. J. Davis, 'All in Good Faith? Proximity, Politicisation, and Malaysia's External Intelligence Organisation', *International Journal of Intelligence and CounterIntelligence*, vol. 32, no. 4, May 2019, pp. 691–716, https://www.tandfonline.com/doi/abs/10.1080/08850607.2019.1621105.

18 Regimen Semboyan Diraja

19 Marhalim Abas, 'Restructuring of the Signals Regiment', Malaysian Defence, 19 November 2019, https://www.malaysiandefence.com/restructuring-of-the-signals-regiment.

20 'Malaysia's digital economy now contributes one fifth to GDP', Consultancy.asia, 7 July 2020, https://www.consultancy.asia/news/3370/malaysias-digital-economy-now-contributes-one-fifth-to-gdp.

21 World Bank Group, 'Malaysia's Digital Economy: A New Driver of Development', September 2018, https://openknowledge.worldbank.org/bitstream/handle/10986/30383/129777.pdf.

22 Malaysia Digital Economy Corporation, 'Who We Are', https://mdec.my/about-mdec/who-we-are.

23 Malaysia Digital Economy Corporation, 'What We Offer', https://mdec.my/what-we-offer/msc-malaysia.

24 Malaysia Digital Economy Corporation, 'A Nation's Commitment to the Digital Economy', https://mdec.my/about-malaysia/government-policies.

25 'MCMC: 43.38 million Broadband Subscription in Malaysia, 82.2% 4G LTE Coverage', Malaysian Wireless, 18 May 2020, https://www.malaysianwireless.com/2020/05/mcmc-fixed-broadband-mobile-subscribers-malaysia.

26 B.K. Sidhu, 'Going beyond fibre for internet throughout Malaysia', *Star*, 28 January 2019, https://www.thestar.com.my/business/business-news/2019/01/28/going-beyond-fibre.

27 Malaysian Communications and Multimedia Commission, 'National Fiberisation and Connectivity Plan', https://www.nfcp.my/Nfcp/media/Docs/NFCP-FS002-v5c.pdf.

28 Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', Medium.com, 20 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-states-stay-ahead-of-china-61cf14b1216.

29 Royce Tan, 'AI Park Will Help Malaysia Take the Lead in Digital Future', *Star*, 17 October 2020, https://www.thestar.com.my/business/business-news/2020/10/17/ai-park-will-help-malaysia-take-the-lead-in-digital-future.

30 *Ibid*.

31 Tenaga Nasional, 'Corporate Profile', https://www.tnb.com.my/about-tnb/corporate-profile.

32 P. Prem Kumar, 'TNB expanding fixed broadband footprint in rural homes', The Malaysian Reserve, 26 November 2018, https://themalaysianreserve.com/2018/11/26/tnb-expanding-fixed-broadband-footprint-in-rural-homes.

33 Telekom Malaysia Berhad, 'Review of the Year & Key Achievements', 2020, https://www.tm.com.my/annualreport/#/review-of-the-year-key-achivements.

34 Fibrecomm Network, 'Company profile', https://www.fibrecomm.net.my/?page_id=10830.

35 Sidhu, 'Going beyond fibre for internet throughout Malaysia'.

36 Alexander Wong, 'Penang is the first state to make fibre optic infrastructure mandatory for new developments', SoyaCincau, 24 December 2020, https://www.soyacincau.com/2020/12/24/penang-fibre-optic-broadband-infrastructure-basic-utility-first-state-malaysia.

37 Caleb Henry, 'Measat buying single replacement for two satellites', SpaceNews, 6 May 2019, https://spacenews.com/measat-buying-single-replacement-for-two-satellites.

38 Computer Crimes Act 1997, Laws of Malaysia, Act 563, http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20563.pdf.

39 See International Telecommunication Union, 'Global Cybersecurity Agenda', https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx. The ITU describes the GCA as 'a framework for international cooperation aimed at enhancing confidence and security in the information society', adding that it was 'designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts'.

40 'Communications and Multimedia Act 1998', Commonwealth Legal Information Institute, http://www.commonlii.org/my/legis/consol_act/cama1998289.

41 Personal Data Protection Act 2010, Laws of Malaysia, Act 709, http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206%202016.pdf.

42 National Cyber Coordination and Command Centre, 'About Us', http://www.nc4.gov.my/about_us.

43 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 38, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

44 National Cyber Coordination and Command Centre, 'About Us'.

45 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 38.

46 Cyber Intelligence, 'Cyber Intelligence (CI)', https://www.cybersecurityintelligence.com/cyber-intelligence-ci-4798.html.

47 CyberSecurity Malaysia, 'Milestones', https://www.cybersecurity.my/en/about_us/milestones/main/detail/2325/index.html.

48 See Chew Kherk Ying, 'Cyber Security 2020, Malaysia', Chambers and Partners, 16 March 2020, https://practiceguides.chambers.com/practice-guides/cybersecurity-2020/malaysia.

49 National Security Council, Prime Minister's Department, 'Malaysia Cyber Security Strategy 2020–2024', pp. 30–9.

50 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 58.

51 Azian Ibrahim et al., 'Cyber Warfare Impact to National Security – Malaysia Experiences', paper presented to FGIC 2nd Conference on Governance and Integrity 2019, Yayasan Pahang, Kuantan, Pahang, Malaysia, 19–20 August 2019, p. 222, https://knepublishing.com/index.php/KnE-Social/article/download/5052/10067.

52 'Malaysia's cybersecurity, forensic labs among most advanced in the world', *Sun Daily*, 27 May 2019, https://www.thesundaily.my/local/malaysia-s-cybersecurity-forensic-labs-among-most-advanced-in-the-world-KM916936.

53 *Cyber Security – Towards a Safe and Secure Cyber Environment*, p. 53.

54 Association of Southeast Asian Nations, 'Co-Chairs' Summary Report – 1st ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies', Kuala Lumpur, 25–26 April 2018, p. 2, http://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ANNEX-12.pdf.

55 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.

56 United Nations General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/70/174, 22 July 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

57 Along with their counterparts from other ASEAN member states, Malaysian officials have participated in training workshops led by, among others, the Australian Strategic Policy Institute (April 2019) and the United Nations Office of Disarmament Affairs in cooperation with the Cyber Security Agency of Singapore (July 2019).

15. Vietnam

Vietnam has put in place a suite of strategies for cyber security and the advancement of its national power in cyberspace, including in the military domain. The governance structures for cyber policy operate through the ruling Communist Party of Vietnam's authoritarian political system. The government has implemented several policies that have contributed to robust growth in the ICT sector and to significant progress in the construction of e-government platforms. However, many government agencies still grapple with cyber-security issues because of a lack of funds and a huge shortage of cyber-security talent. The Communist Party's concerns regarding the threat of internal subversion probably draw resources away from technical cyber-skills training and towards ideological work and the management of public opinion, thereby reducing investment in both defensive and offensive cyber capabilities. While overall offensive cyber capabilities are likely to be nascent or weak, the covert government-linked group APT32 could probably launch relatively sophisticated cyber attacks. Vietnam is a third-tier cyber power but it has considerable digital ambition and potential. If it can strengthen its key cyber-security skills, support its ICT firms and invest in advanced technology to protect its digital infrastructure, it could realise that potential.

Strategy and doctrine

Vietnam's laws and regulations surrounding cyber security were rather disparate until 2010, when it released its first national road map, 'Approving the National Planning on Development of Digital Information Security'.[1] The plan was more comprehensive and ambitious than those that most other countries had produced by that point. Its four overarching goals, aimed at addressing technical and legal weaknesses in the country's information security, were: to ensure the security of network and information infrastructure; to ensure the safety of data and applications; to train cyber-security professionals and increase public awareness of information security; and to enhance the legal framework for information security, especially relating to computer crime and encryption. Funding was provided to train personnel in state agencies and bolster information security in the Ministry of Information and Communications (MIC), the Ministry of Public Security (MPS), the Government Cipher Committee and the Ministry of Industry. The road map also identified the need to encourage research and development (R&D).

A Network Information Security Plan was launched in 2016, aiming to augment the 2010 road map by outlining further objectives for the period 2016–20.[2]

List of acronyms

AIS	Authority of Information Security
ASEAN	Association of Southeast Asian Nations
CPV	Communist Party of Vietnam
ICT	information and communications technology
MIC	Ministry of Information and Communications
MND	Ministry of National Defence
MPS	Ministry of Public Security
NCSC	National Cyber Security Monitoring Centre
NSCER	National Steering Committee for Emergency Response
VNCERT	Vietnam Computer Emergency Response Team
VNPT	Vietnam Posts and Telecommunications Group
VPA	Vietnamese People's Army

It emphasised R&D and governmental cooperation with Vietnamese information-security firms through outsourcing, and set targets for the establishment of home-grown brands of information-security products. Vietnamese ICT associations were identified as key players in promoting this initiative.[3] The plan also advocated the nationwide coordination of responses to security incidents. It foreshadowed the development of minimum security requirements for key national systems (both critical infrastructure and more sensitive government communications). Individual companies would be obliged to take responsibility for security by adhering to the relevant regulations, and to submit to regular audits of this compliance. The plan also promoted cyber-security drills for government- and private-sector entities, along with their participation in international forums.

For the Vietnamese government, cyber security is not just a technical question of protecting networks but also involves controlling the political content carried by those networks – as demonstrated, for example, by the Law on Network Information Security passed in November 2015.[4] While this law focused primarily on technical and management aspects of preventing unauthorised access to ICT systems, it made clear that censorship and monitoring of domestic political expression would be a high priority for the government. It also flagged the need to control international exchanges in cyberspace, defining as illegal any information-related activity that the government considered a threat to national security, whether carried out by Vietnamese or foreign entities.

The Cyber Security Law passed in June 2018 was even more overtly political in its purpose, aiming to protect national security and ensure 'social order and safety in cyberspace' (Article 1).[5] It included extensive definitions around content acceptability that were not part of the 2015 law. For example, in Article 8, it described as 'strictly prohibited' any attempt to 'oppose the State' or to distort history by 'denying revolutionary achievements'. One of the most controversial elements of the 2018 law was enforced data localisation[6] for all domestic and foreign companies operating in Vietnam, a move seen by the foreign companies as infringing on their business confidentiality and intellectual-property rights.[7]

The first official public document to convey Vietnam's perspective on applying cyber to the military domain was the National Defence Law, also introduced in 2018.[8] It described 'information warfare' as 'activities and measures to disable the enemy's information systems and secure Vietnam's information systems', which it included in the concept of 'all-people national defense' (Article 2), and specifically mentioned both cyber warfare and information warfare. The same year saw a Politburo resolution announcing a new 'Strategy for the Homeland Protection in Cyberspace',[9] designed to develop a whole-of-society response, though centred on the armed forces, and to combine cyber defence with counter-attack.[10]

A defence white paper published in 2019 presented cyberspace as the fifth operational domain – alongside land, air, sea and space – in which to defend Vietnam's national sovereignty.[11]

Governance, command and control

Security policy, including for cyberspace, is directed by the Politburo of the Communist Party of Vietnam (CPV). The armed forces, through their Cyber Command, have a more central role in censorship and political surveillance than is the case in most countries, and therefore the Central Military Commission of the CPV, Vietnam's highest decision-making body for national security, is probably the main command and governance authority for cyberspace policy. Other departments close to the party leadership, such as the Propaganda Department, also play a role in dealing with the most sensitive security issues.

The cyber policies dictated by the CPV leadership are implemented primarily by the MIC, the MPS and the Ministry of National Defence (MND), with the MIC as the coordinator for more technical aspects of cyber security as well as broad policies on content management.[12] Within the MIC, the Vietnam Computer Emergency Response Team (VNCERT)[13] coordinates nationwide incident-response activities, collects and shares information on incidents and malware, directs cyber operations, and undertakes the testing of the cyber defences of public- and private-sector entities.[14] The Authority of Information Security (AIS) formulates laws and policies regarding information security, and implements technical

measures to protect critical information infrastructure,[15] while the National Electronic Authentication Centre secures electronic transactions through digital signatures and other authentication services.[16]

The MPS has two cyber-security departments – Cyber Security and High-tech Crime Prevention (A05), and Information Security and Communications (A87). A05 is tasked with preventing cyber crime, including online gambling and the spreading of false information, and cooperates with foreign investigation agencies on cases involving foreign cyber criminals. It also provides advice on cyber-security laws and policies, and promotes high-tech solutions aimed at boosting the government's capacity to counter cyber crime.[17] A87 plays an advisory role on matters of policy, on legal aspects of security in the fields of culture, information and communication, and on countering criticism of the CPV and the leaking of state secrets.[18]

The MND directs two cyber-security departments – Cyber Command and the Government Cryptographic Agency. Cyber Command, established in August 2017 as an upgrade of the former Information Technology Department, reports to the Chief of the General Staff, who in turn is subordinate to the defence minister (a Politburo member). Comprising the Command Headquarters, three brigades, testing centres and a data centre, its responsibilities include political work, technical and logistical issues, and professional cyber operations.[19] The Government Cryptographic Agency is in charge of securing the state's encrypted networks and R&D of related technologies.[20]

The Vietnamese People's Army (VPA) contains a special cyber unit, Force 47, tasked with protecting the CPV against 'false news' and disseminating state propaganda. It has a task force whose personnel, numbering more than 10,000,[21] have received training in ideological discipline and information warfare.[22] They often operate on social-media platforms, including Facebook and YouTube, aiming to pre-empt any spreading of hostile information prior to major political events.

There is not enough information in the public domain to allow a confident assessment of the effectiveness of the governance and command arrangements for Vietnam's cyber forces, beyond the observation that strict obedience to the chain of command is enforced.

Core cyber-intelligence capability

Vietnam's cyber-intelligence capabilities lie in the MPS, MND and MIC. Within the MPS, the General Department of Intelligence and the General Department of Security (GDS) collect domestic and foreign intelligence. Inside the GDS, the specialist unit A42 monitors telephone calls, emails and the internet using systems procured from foreign vendors.[23] Also within the MPS, the Department for Cyber Security and High-tech Crime Prevention (AO5 – see previous section) has invested in modern technical equipment[24] and has joined Microsoft's Government Security Program to enhance its awareness of cyber threats.[25]

Within the MND, the General Department of Military Intelligence is responsible for domestic and foreign intelligence. Cyber Command, although not an intelligence agency, is likely to possess cyber-intelligence capabilities that would have evolved from the VPA's proven signals-intelligence capacity during the Vietnam War. Also operating within the MND, the Government Cryptographic Agency is a vital part of Vietnam's cyber-intelligence capability, being responsible for ensuring the cyber security of the country's civilian and military leaders.

In its role as coordinator for all government departments concerned with cyber security, the MIC also possesses cyber-intelligence capabilities. Its National Cyber Security Monitoring Centre works alongside the VNCERT and provincial Cyber Security Control Centres[26] in monitoring Vietnamese cyberspace for potential threats.

Vietnam's cyber-intelligence capability is amplified to some degree by a group known to cyber-security companies as APT32.[27] Though apparently a non-state entity, it is assessed to have informal links to the government. Its cyber-espionage operations have been widely documented by US cyber-security companies and appear to have been quite proficient, with targets including foreign companies, the Association of Southeast Asian Nations (ASEAN) and Chinese government institutions (including those managing China's response to COVID-19). Overall, however, Vietnam's cyber-intelligence capability is likely to be weak, in part because of the country's shortage of skilled workers in the ICT domain.[28]

Cyber empowerment and dependence

In 2019 the Politburo announced the target that Vietnam's digital economy should contribute 20% of GDP by 2025 and at least 30% by 2030,[29] as compared with 15% in 2018.[30] This will only be achievable with significant policy reform and large-scale new investment. The government has been pushing forward initiatives such as the National Digital Transformation Programme, launched in 2020,[31] and has prioritised e-government projects.[32] It also claims that the ICT sector has been growing at an impressive average annual rate of 30% for a number of years (the precise period is not stated).[33] However, in almost all indicators of ICT readiness, Vietnam ranks behind Malaysia and far behind Singapore, though just ahead of Indonesia.[34] In 2020 the country's internet penetration rate reached 70%[35] and its e-commerce market was the third biggest in Southeast Asia, just behind those in Indonesia and Thailand.[36] Though significant progress has been made, there is still some way to go in terms of digital transformation. For example, cashless payments account for only a small proportion of total payments, and cash-on-delivery payment methods are preferred even for e-commerce transactions.[37]

In the field of artificial intelligence (AI), Vietnam fared quite well in a ranking of the top 50 countries based on their contributions to the two most prestigious AI conferences in 2020: it was placed 27th, ahead of Malaysia and Thailand but behind Singapore.[38] The same study compiled a ranking of the global top 100 companies in AI research in 2020: it was dominated by US and Chinese companies but Vietnam's VinAI was also included, in 32nd place.[39] Founded by a former employee of Google DeepMind, VinAI provides applied AI solutions and is also the first Vietnamese research laboratory to cover areas such as machine learning and deep learning.[40] AI has already been applied in sectors such as healthcare, education, transport, agriculture and e-commerce, though overall it is still in the early stages of development.[41] The government announced a ten-year strategy for AI R&D in January 2021, setting the goal of becoming one of the world's top 50 countries in the field by 2030.[42]

Vietnam has a reasonable degree of national ownership of its telecommunications networks, owning about 75% of the equipment, and hopes to achieve 100% domestic production of that equipment by 2022.[43] Viettel, a military-owned telecoms carrier, is part of a consortium developing a high-performance undersea cable, capable of carrying more than 140 Tb/s of traffic, that will connect China (Hong Kong and Guangdong), Japan, the Philippines, Singapore, Thailand and Vietnam as part of the Asia Direct Cable project, due to be completed by the end of 2022.[44] It has also successfully tested 5G technology.[45] Vietnam Posts and Telecommunications Group (VNPT) exports to more than 30 countries.[46]

Vietnam has a reasonable degree of national ownership of its telecommunications networks

In terms of space-based connectivity, VNPT operates two communications satellites, VINASAT-1 and VINASAT-2.[47] Vietnam also has two Earth-observation satellites, operated by the Vietnam National Space Centre (VNSC) and the Space Technology Institute of the Vietnam Academy of Science and Technology. The space industry relies heavily on foreign assistance and investment – for example, Japanese experts were involved in building one of the Earth-observation satellites, the VNSC's *MicroDragon*, launched from Japan in 2019,[48] and India has been collaborating with Vietnam's National Remote Sensing Department in building a tracking and telemetry station that potentially has military uses.[49]

Cyber security and resilience

Vietnam has been constructing an elaborate set of mechanisms, policies and laws for national cyber security for over a decade. The efforts have paid off to some degree but there is much progress still to be made. According to Microsoft reporting in 2020, the country had the highest rate of ransomware attacks in the Asia-Pacific, it was one of the three countries in the region most affected by malware attacks[50] and it ranked sixth in the world for unintentional downloads of malicious code.[51]

In response to the growing cyber threats, the National Cyber Security Monitoring Centre[52] (NCSC) was established under the AIS in 2018. Its primary focus is to support and supervise the cyber security of

all public- and private-sector entities, to provide early warnings against cyber attacks, and to share information with domestic and international agencies. In partnership with a coalition of information-security companies, the NCSC has launched an information-sharing and security-monitoring system that connects the ministries of the central government with the country's provincial administrations.[53] In 2020, for example, it cooperated with the MIC and MPS in containing the VN84App spyware that was targeting smartphone users.[54]

In terms of overall national resilience, it is difficult to form a clear picture. The 'Strategy for the Homeland Protection in Cyberspace'[55] and its implementation plan would appear to be the main policy document setting out the response plans for serious cyber incidents, but the texts are not available. Vietnam responds to such incidents through the National Steering Committee for Emergency Response (NSCER),[56] which the MIC assists by directing and coordinating emergency-response efforts domestically or internationally.[57] The VNCERT is responsible for responding to lower-level cyber incidents but participates in the NSCER along with cyber-related agencies in the MIC, MPS and the MND. The VNCERT also works with other, smaller CERTs at the ministerial, provincial and local levels; with enterprises engaged in telecommunications, internet services, data storage, banking and financial activities; and with organisations that manage critical information infrastructure or industrial control systems.[58] In 2019 VNCERT conducted a nationwide cyber-security exercise with almost 300 participants.[59]

The private sector has been playing an increasing role in promoting information security, including by creating its own cyber-security industry – for example, Viettel has created a subsidiary providing managed cyber-security services;[60] VNPT conducts cyber-security research and invests in relevant start-ups; and eight companies have come together to form the Vietnam Cyber Security Assessment and Audit Club, aiming to improve the assessment and auditing of cyber-security services nationwide.

Overall, however, Vietnam still faces significant cyber-security challenges. It remains to be seen whether the NSCER is capable of coordinating effectively across the public and private sectors. The MIC has stated that there are not enough trained personnel to create the necessary CERTs and that the emergency-response network is 'unconnected' and 'unprofessional'.[61] Investments in research and training that were approved in 2014 have yet to be implemented;[62] a 2019 study suggested that almost half of government agencies lacked the funds necessary to implement cyber security;[63] and in 2020, reporting on its campaign to upgrade cyber security, the government noted that 30% of ministries had not yet reached the target level.[64] Vietnam ranked 50th out of 175 countries in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union.[65]

Global leadership in cyberspace affairs

Vietnam focuses its cyber diplomacy on ASEAN, enthusiastically promoting cyber-security cooperation between members and with the group's external partners. Under the ASEAN Plus Three framework, for example, Hanoi hosted a December 2020 meeting with China, Japan and South Korea on international collaboration in cyber security and countering cyber crime.[66] Within ASEAN, Vietnam works actively towards cooperation on cyber norms[67] and the creation of a formal cyber-security cooperation mechanism.[68] The VNCERT hosted the June 2020 ASEAN–Japan Cyber Exercise, which focused on methods for countering fake websites.[69]

Vietnam still faces significant cyber-security challenges

Vietnam frequently collaborates with foreign governments and corporations to broaden its cyber-security capabilities. In 2019, for example, the NCSC signed a contract with Kaspersky to address information-security challenges,[70] and in 2020 the MPS collaborated with India,[71] Brunei[72] and Malaysia[73] on countering cyber crime. The country is part of the global Forum of Incident Response and Security Teams and the Asia-Pacific Computer Emergency Response Team (APCERT).[74] It has privately expressed an interest in close collaboration with the United States and Australia in matters of cyber security, but there are diplomatic obstacles because of human-rights concerns regarding Vietnamese cyber-security law. Nevertheless, both the

US and Australia undertake activities with Vietnam in less sensitive areas of cyberspace policy such as international legal training and the development of smart cities.

Offensive cyber capability

It is unlikely that Vietnam's Cyber Command is well positioned to engage in offensive cyber operations against foreign adversaries, given its extensive domestic political roles and responsibilities and, according to its chief of staff, its lack of appropriate facilities, equipment and cyber weapons.[75] Force 47 probably does not possess the technical abilities for significant offensive cyber because its mission is primarily political, mainly involving the management of public opinion by countering hostile viewpoints and creating propaganda.[76] The covert government-linked group APT32 is mainly engaged in industrial and other types of espionage rather than offensive cyber, but it probably possesses some capabilities that could be repurposed for an offensive effect. Overall, developing an offensive cyber capability does not appear, so far, to have been a high priority for the CPV.

Notes

1 Prime Minister's Decision No. 63/QD-TTg, 'Approving the National Planning on Development of Digital Information Security through 2020', 2010, https://vanbanphapluat.co/decision-no-63-qd-ttg-approving-the-national-planning-on-development-of-digital-information-security-through-2020.

2 Prime Minister, 'Phê Duyệt Phương Hướng, Mục Tiêu, Nhiệm Vụ Bảo Dảm An Toàn Thông Tin Mạng Giai Doạn 2016–2020', 27 May 2016, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-898-QD-TTg-phuong-huong-muc-tieu-nhiem-vu-bao-dam-an-toan-thong-tin-mang-2016-2020-313149.aspx.

3 Key players in promoting the Vietnamese information-security industry include the Vietnam Software and IT Services Association, the Vietnam Association for Information Processing, the Vietnam Internet Association, the Vietnam Information Security Association and the Vietnam E-commerce Association.

4 National Assembly, 'Luật an toàn thông tin mạng', 86/2015/QH13, 19 November 2015. For an official translation, see https://vanbanphapluat.co/law-no-86-2015-qh13-on-cyberinformation-security-2015.

5 National Assembly, 'Luật An Ninh Mạng', 24/2018/QH14, 12 June 2018, https://luatvietnam.vn/an-ninh-quoc-gia/luat-an-ninh-mang-2018-164904-d1.html. For an unofficial translation, see https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf.

6 Thomas J. Treutler and Giang Thi Huong Tran, 'Update on the Implementation of Vietnam's New Cybersecurity Law and Status of Implementing Decrees', Tilleke & Gibbins, 18 December 2019, https://www.lexology.com/library/detail.aspx?g=8833627c-e189-4d60-a472-6ee742cc38fd.

7 The data-localisation obligation for foreign companies applies to those that provide telecoms services, data storage and sharing, e-commerce, social media and online electronic games.

8 National Assembly, 'Luật Quốc Phòng', 22/2018/QH14, 8 June 2018, https://thuvienphapluat.vn/van-ban/bo-may-hanh-chinh/Luat-quoc-phong-340395.aspx.

9 Politburo Resolution 29NQ/TW dated 25 July 2018. See Vu Van Hien, 'Enhancing the homeland protection under the Party's platform', *National Defence Journal*, 10 November 2020, http://tapchiqptd.vn/en/theory-and-practice/enhancing-the-homeland-protection-under-the-partys-platform/16265.html; and Ngo Xuan Lich, 'The whole military resolves to successfully fulfil the military-defence tasks in 2019', *National Defence Journal*, 4 January 2019, http://tapchiqptd.vn/en/theory-and-practice/the-whole-military-resolves-to-successfully-fulfil-the-militarydefence-tasks-in-2019/13088.html.

10 Ngoc Thuy Tran, 'Những Vấn Dề về Bảo vệ Tổ Quốc Trên Không Gian Mạng', Quan khu 7, 3 October 2019, https://baoquankhu7.vn/nhung-van-de-ve-bao-ve-to-quoc-tren-khong-gian-mang--191939649-00150445340108s.

11 Ministry of National Defence, '2019 Viet Nam National Defence', October 2019, p. 52, http://news.chinhphu.vn/Uploaded_VGP/phamvanthua/20191220/2019VietnamNationalDefence.pdf.

12 National Assembly, 'Luật An Ninh Mạng', 24/2018/QH14.

13 See 'VNCTERT/CC Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam', http://vncert.gov.vn.

14 Ministry of Information and Communications, 'Cybersecurity Emergency Response Center established', 14 October 2019, https://

english.mic.gov.vn/Pages/TinTuc/139865/Cybersecurity-Emergency-Response-Center-established.html.

15 Ministry of Information and Communications, 'Authority of Information Security', 19 July 2020, https://english.mic.gov.vn/pages/thongtin/114301/Authority-of-Information-Security.html.

16 Ministry of Information and Communications, 'The National Electronic Authentication Centre', 19 July 2020, https://english.mic.gov.vn/pages/thongtin/114304/NEAC.html.

17 'Chủ động, quyết liệt trong phòng, chống tội phạm trên không gian mạng', Thua Thien Hue Provincial Party Committee, 21 January 2020, https://tinhuytthue.vn/tin-tuc-trong-nuoc/kh-cn/chu-dongquyet-liet-trong-ph-ograve-ngchong-toi-pham-tr-ecirc-n-kh-ocirc-ng-gian-mang.htm.

18 'Cục An ninh Văn hóa, thông tin, truyền thông báo công dâng Bác', *Tiền Phong*, 5 May 2018, https://www.tienphong.vn/xa-hoi/cuc-an-ninh-van-hoa-thong-tin-truyen-thong-bao-cong-dang-bac-1269610.tpo.

19 Ministry of National Defence, '2019 Viet Nam National Defence'.

20 *Ibid*., pp. 66–7.

21 'Hơn 10.000 người trong 'Lực lượng 47' dấu tranh trên mạng', *Tuổi Trẻ*, 25 December 2017, https://tuoitre.vn/hon-10-000-nguoi-trong-luc-luong-47-dau-tranh-tren-mang-20171225150602912.htm. It is unclear from this source if the personnel engage only in political surveillance or if some also conduct other cyber operations.

22 Maj. Gen., Associate Prof. Nguyen Hung Oanh, 'The Political Officer College grasps and executes the Politburo's Resolution 35', *National Defence Journal*, 16 October 2019, http://tapchiqptd.vn/en/research-and-discussion/the-political-officer-college-grasps-and-executes-the-politburos-resolution-35/14514.html.

23 Carlyle A. Thayer, 'The Apparatus of Authoritarian Rule in Vietnam', *Critical Studies of the Asia Pacific Series*, vol. 31, no. 2, 2014, pp. 279–83, https://link.springer.com/chapter/10.1057/9781137347534_7#aboutcontent.

24 Hai Thanh Luong et al., 'Understanding Cybercrimes in Vietnam: From Leading-Point Provisions to Legislative System and Law Enforcement', *International Journal of Cyber Criminology*, vol. 13, no. 2, 2019, https://www.cybercrimejournal.com/LuongetalVol13Issue2IJCC2019.pdf.

25 'VN to join Microsoft's network security protection programme', *Viêt Nam News*, 20 December 2019, https://vietnamnews.vn/society/570139/vn-to-join-microsofts-network-security-protection-programme.html.

26 Le Linh, 'Xây dựng trung tâm diều hành an ninh mạng đầu tiên cả nước', Diễn Dàn, 17 May 2019, https://enternews.vn/xay-dung-trung-tam-dieu-hanh-an-ninh-mang-dau-tien-ca-nuoc-150441.html.

27 For some background, see Nick Carr, 'Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations', FireEye, 14 May 2017, https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html.

28 Tran Luu, 'Vietnam determines to develop digital economy', Saigon Online, 4 February 2020, https://sggpnews.org.vn/science_technology/vietnam-determines-to-develop-digital-economy-85491.html.

29 Bui Thanh Truan, 'Difficulties and challenges in the development of digital economy in Vietnam', Political Theory, 25 August 2020, http://lyluanchinhtri.vn/home/en/index.php/practice/item/723-difficulties-and-challenges-in-the-development-of-digital-economy-in-vietnam.html.

30 Chinese Academy of Information and Communications Technology, 'Quánqiú shùzì jīngjì xīn túijīng (2019 nián)', October 2019, p. 12, http://www.caict.ac.cn/kxyj/qwfb/bps/201910/P020191011314794846790.pdf.

31 See Prime Minister, 'Introducing Program for National Digital Transformation by 2025 with Orientations Towards 2030', Decision 749/QD-TTg, 3 June 2020, https://vanbanphapluat.co/decision-749-qd-ttg-2020-introducing-program-for-national-digital-transformation. By 2030 this programme aims to achieve the following: a digital economy that contributes 30% of GDP; digital transformation in the government sector so that Vietnam becomes one of the top four ASEAN countries in the UN e-government ranking; nationwide 5G mobile-network coverage; and access to broadband internet for the entire population.

32 Samaya Dharmaraj, 'Vietnam Committed to Supporting its Digital Economy with E-government', OpenGov Asia, 28 November 2019, https://www.opengovasia.com/vietnam-committed-to-supporting-its-digital-economy-with-e-government.

33 Ministry of Information and Communications, 'VN's IT industry maintains growth momentum', 25 December 2019, https://english.mic.gov.vn/Pages/TinTuc/140438/VN-s-IT-industry-maintains-growth-momentum.html.

34 George Ingram, 'Development in Southeast Asia: Opportunities for donor collaboration', Brookings Center for Sustainable Development, December 2020, pp. 31–2, https://www.brookings.edu/wp-content/uploads/2020/12/Development-Southeast-Asia-Ch2-Digital.pdf.

35 Simon Kemp, 'Digital 2020: Vietnam', DataReportal, 18 February 2020, https://datareportal.com/reports/digital-2020-vietnam.

36 'How can Vietnam's e-commerce players foster greater market growth?', Tech Wire Asia, 3 February 2020, https://techwireasia.com/2020/02/how-can-vietnams-e-commerce-players-foster-greater-market-growth.

37 'Cashless payment remains low in Vietnam: CIEM', VietnamPlus, 24 June 2019, https://en.vietnamplus.vn/cashless-payment-remains-low-in-vietnam-ciem/154911.vnp.

38 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.

39 *Ibid.*

40 'Who We Are – The First AI Research Lab in Vietnam with a Focus on Fundamental Research', VinAI Research, https://www.vinai.io/about-us.

41 'Vietnam Prioritises Artificial Intelligence Development', *Star*, 9 September 2019, https://www.thestar.com.my/business/smebiz/2019/09/09/vietnam-prioritises-artificial-intelligence-development.

42 'Vietnam strives to enter world's Top 50 in terms of AI by 2030', VietnamPlus, 28 January 2021, https://en.vietnamplus.vn/vietnam-strives-to-enter-worlds-top-50-in-terms-of-ai-by-2030/195485.vnp.

43 'Việt Nam nhờ Mỹ kiểm định thiết bị 5G do Việt Nam sản xuất để có dủ khả năng vào thị trường Mỹ', ICT News, 21 January 2020, https://ictnews.vietnamnet.vn/cuoc-song-so/viet-nam-nho-my-kiem-dinh-thiet-bi-5g-do-viet-nam-san-xuat-de-co-du-kha-nang-vao-thi-truong-my-40145.html.

44 Ministry of Information and Communications, 'Viettel among investors of new high-speed under-sea cable ADC', 22 June 2020, https://english.mic.gov.vn/Pages/TinTuc/142715/Viettel-among-investors-of-new-high-speed-under-sea-cable-ADC.html.

45 Leo Kelion, 'Giới chuyên gia ngạc nhiên trước tuyên bố của Viettel về mạng 5G', BBC News Vietnamese, 21 January 2020, https://www.bbc.com/vietnamese/vietnam-51190570.

46 'Vietnamese telecom giants on race of exporting telecom equipments', Xinhua, 24 February 2017, http://www.xinhuanet.com//english/2017-02/24/c_136082932.htm.

47 Union of Concerned Scientists, 'UCS Satellite Database', updated 1 January 2021, https://www.ucsusa.org/resources/satellite-database.

48 'Vietnam's MicroDragon Earth Observation Satellite Successfully Launched From Japan', SpaceWatch Asia Pacific, January 2019, https://spacewatch.global/2019/01/vietnams-microdragon-earth-observation-satellite-successfully-launched-from-japan.

49 Nandini Sarma, 'Southeast Asian Space Programmes: Capabilities, challenges and collaborations', Observer Research Foundation, 7 March 2019, https://www.orfonline.org/research/southeast-asian-space-programmes-capabilities-challenges-collaborations-48799/#_ednref12.

50 M. Anh, 'Việt Nam là quốc gia có tỷ lệ nhiễm mã độc tống tiền cao nhất khu vực', *Doanh nhân*, 24 June 2020, https://doanhnhansaigon.vn/it/viet-nam-la-quoc-gia-co-ty-le-nhiem-ma-doc-tong-tien-cao-nhat-khu-vuc-1099286.html.

51 Microsoft, 'Microsoft Security Endpoint Threat Summary 2019', June 2020, https://3er1viui9wo30pkxh1v2nh4w-wpengine.netdna-ssl.com/wp-content/uploads/prod/sites/570/2020/02/Microsoft-Security-Endpoint-Threat-Summary-2019-Updated.pdf.

52 See 'Giới thiệu về NCSC', National Cyber Security Monitoring Centre, https://khonggianmang.vn/intro.

53 Phan Nghia, 'Vietnam introduces new information security system to facilitate e-governance', *VnExpress*, 29 November 2019, https://e.vnexpress.net/news/news/vietnam-introduces-new-information-security-system-to-facilitate-e-governance-4019639.html.

54 Bao Lam and Chau An, 'Data stealing spyware rears head in Vietnam', VnExpress, 23 June 2020, https://e.vnexpress.net/news/news/data-stealing-spyware-rears-head-in-vietnam-4119828.html.

55 Vu, 'Enhancing the homeland protection under the Party's platform'; Ngo, 'The whole military resolves to successfully fulfil the military-defence tasks in 2019'.

56 Prime Minister, 'Quyết Định: Ban Hành Quy Định Về Hệ Thống Phương Án Ứng Cứu Khẩn Cấp Bảo Dảm An Toàn Thông Tin Mạng Quốc Gia', 05/2017/QD-TTg, 16 March 2017, https://vanbanphapluat.co/quyet-dinh-05-2017-qd-ttg-he-thong-phuong-an-ung-cuu-khan-cap-bao-dam-an-toan-thong-tin-mang-quoc-gia.

57 'PM sets up national cybersecurity committee', *Vietnam Law & Legal Forum*, 2 April 2017, https://vietnamlawmagazine.vn/pm-sets-up-national-cybersecurity-committee-5785.html.

58 Prime Minister, 'Quyết Định: Ban Hành Quy Định Về Hệ Thống Phương Án Ứng Cứu Khẩn Cấp Bảo Dảm An Toàn Thông Tin Mạng Quốc Gia'.

59 'Vietnam records more than 6,200 cyber attacks in seven months', AsiaOne, 1 August 2019, https://www.asiaone.com/digital/vietnam-records-more-6200-cyber-attacks-seven-months.

60 'The first information security ecosystem built by Vietnamese', Acrofan, 20 February 2020, https://us.acrofan.com/detail.php?number=239640.

61 Samaya Dharmaraj, 'Vietnam strengthens human resources for information security tasks', OpenGov Asia, 9 July 2019, https://www.opengovasia.com/vietnam-strengthens-human-resources-for-information-security-tasks.

62 *Ibid*.

63 Chau An, 'Vietnam carries potential to be a cybersecurity powerhouse: minister', VnExpress, 17 April 2019, https://e.vnexpress.net/news/business/economy/vietnam-carries-potential-to-be-a-cybersecurity-powerhouse-minister-3910754.html.

64 'Cyber attacks targeting Vietnam's information systems down 7.8 pct', VietnamPlus, 4 November 2020, https://en.vietnamplus.vn/cyber-attacks-targeting-vietnams-information-systems-down-78-pct/189811.vnp.

65 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 63, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

66 Ministry of Public Security, 'Asean +3 conference on cyber security opens in Hanoi', 29 December 2020, http://en.bocongan.gov.vn/international-relations-cooperation/asean-3-conference-on-cyber-security-opens-in-hanoi-t7615.html.

67 Li Ying Lee, 'New ASEAN committee to implement norms for countries' behaviour in cyberspace', Channel News Asia, 2 October 2019, https://www.channelnewsasia.com/news/singapore/asean-cyberspace-working-level-committee-cybersecurity-11963602.

68 'ASEAN Member States Agree to Move Forward on a Formal Cybersecurity Coordination Mechanism', CSA Singapore, 2 October 2019, https://www.csa.gov.sg/news/press-releases/amcc-release-2019.

69 'Vietnamese tech experts join transnational cyber-attack exercise', *Viêt Nam News*, 26 June 2020, https://vietnamnews.vn/society/748743/vietnamese-tech-experts-join-transnational-cyber-attack-exercise.html.

70 'National Cyber Security Center signs deal with Kaspersky for online security', VietNamNet, 24 January 2019, https://english.vietnamnet.vn/fms/science-it/216749/national-cyber-security-center-signs-deal-with-kaspersky-for-online-security.html.

71 'Vietnam–India strategic partnership in the fields of defence and security', *National Defence Journal*, 29 August 2017, http://tapchiqptd.vn/en/events-and-comments/vietnam-india-strategic-partnership-in-the-fields-of-defence-and-security/10541.html.

72 'Việt Nam, Brunei, boost co-operation in combating crimes', *Viêt Nam News*, 14 February 2020, https://vietnamnews.vn/politics-laws/592275/viet-nam-brunei-boost-co-operation-in-combating-crimes.html.

73 Ministry of Public Security, 'Vietnam, Malaysia promote cooperation in security', 14 February 2020, http://en.bocongan.gov.vn/international-relations-cooperation/vietnam-malaysia-promote-cooperation-in-security-t6508.html.

74 Adam Bannister, 'APCERT holds cyber drill to stress-test response capabilities of 32 CSIRTs', The Daily Swig, 6 April 2020, https://portswigger.net/daily-swig/apcert-holds-cyber-drill-to-stress-test-response-capabilities-of-32-csirts.

75 'Xây dựng lực lượng Tác chiến không gian mạng, dáp ứng yêu cầu nhiệm vụ bảo vệ Tổ quốc', *Tạp chí Quốc phòng*, 17 October 2019, http://tapchiqptd.vn/vi/bao-ve-to-quoc/xay-dung-luc-luong-tac-chien-khong-gian-mang-dap-ung-yeu-cau-nhiem-vu-bao-ve-to-quoc/14505.html.

76 'Hơn 10.000 người trong 'Lực lượng 47' Dấu tranh trên mạng', *Tuổi Trẻ*.

Net Assessment

Based on the country studies in the report, we can draw conclusions about the ways in which states have responded to the opportunities and threats presented by cyber capabilities. In addition to considering separately each of the categories in our methodology, we can also draw conclusions about the relative standing of the 15 countries and the implications for the broader global balance of power.

Foundations of cyber power

On published *strategy and doctrine*, the country studies reveal considerable variation in practice, especially on the balance between policies for cyber security on the one hand and policies for intelligence-related, political and military uses of cyber assets on the other. All countries maintain high levels of secrecy around the latter three areas. All the countries studied in this report now have some published strategy, doctrine or policy in at least one of the diverse aspects of cyber power. The United States led the way by publishing cyber policies from the mid-1990s onwards. It now has the most mature and comprehensive policy settings. While some other states also produced discrete elements of strategic and doctrinal cyber thinking in the 1990s, it was not until the late 2000s that the first wave of policies comparable in breadth and depth to those of the US were produced. This was followed by a second wave from 2015 onwards. Each study reveals a unique blend of civilian and military elements, reflecting the particular strategic circumstances and policy preoccupations of that country. Given the rapidly evolving nature of cyber threats and opportunities, none of the countries studied is comfortable with its level of maturity on strategy.

National differences also play out in the arrangements for *governance, command and control*. Here, the political culture of each country is immediately visible as the primary determinant of governance arrangements. Liberal democracies in advanced economies such as France, Japan, the United Kingdom and the US tend to have more well-established arrangements for cyber governance compared with democracies in the wealthier developing countries (India, Indonesia and Malaysia). In the latter group, governance arrangements have developed more slowly and unevenly, as have security strategies for cyberspace. In more authoritarian countries such as China, Iran, North Korea and Russia, the governance arrangements are more narrowly focused and less transparent. Of those four countries, only China might be said to have an established framework for a multi-stakeholder approach to cyber governance, although its political system favours the Chinese Communist Party as the dominant stakeholder.

A *core cyber-intelligence capability* is the primary foundation of cyber power. Any country's ability to take defensive or offensive action in cyberspace is fundamentally dependent on its understanding of the cyber environment – its cyber situational awareness. This can be constructed by combining all available sources of information from across the private and public sectors. The most effective intelligence agencies must also have the capability to detect and attribute sophisticated state-based cyber attacks and to conduct sophisticated cyber operations of their own. While many states around the world have cyber capabilities focused on their own internal security, and some have developed a regional intelligence footprint, only a few have sufficient reach to achieve the level of global cyber understanding essential for the most sophisticated operations. Those states are the Five Eyes intelligence allies (Australia, Canada, New Zealand, the UK and the US), which operate

collectively; their two most cyber-capable partners, Israel and France, whose indigenous capabilities are significantly amplified by those of their allies; and China and Russia. In the case of every cyber-capable state, the intelligence agencies have tended to dominate the formulation of national strategy and policy, having a particularly strong influence over the military's approach to offensive cyber. Overall, for all the countries studied in this report, the centrality of highly sensitive intelligence capabilities to cyber operations imposes severe restrictions on the amount of publicly available information regarding many aspects of cyber policy.

In all the country studies, the analysis of *cyber empowerment and dependence* reveals tensions between the globalised character of the ICT sector and national ambitions for domestic industrial development. Israel and Malaysia provide interesting examples of small countries taking ambitious steps to bridge this divide. In the case of the high-tech industries that underpin cyberspace, US geopolitical influence is heightened by the fact that it is home to so many of the dominant companies and that most of the other leading companies are from countries that are US allies. The only state contesting this situation is China, whose share of the global ICT market is growing significantly. All states are grappling with the risks arising from the presence of foreign equipment in their national networks, with indications that a protectionist, risk-averse approach may be unrealistic and potentially self-defeating. The challenges are exacerbated by increasing competition between states in emerging breakthrough technologies such as quantum computing and artificial intelligence (AI).

On *cyber security and resilience*, the most cyber-capable states are developing whole-of-society responses that involve close partnership between the private and public sectors and academia, and between the military and civil sectors, along with efforts aimed at raising public awareness and expanding the skilled workforce. There is considerable variation in the range and effectiveness of measures from country to country, with some attempting top-down approaches directed by the government while others pursue more federated approaches with diverse nodes of initiative and authority. All states seem to recognise the importance of nurturing their cybersecurity companies so that they come to form an effective industrial sector, but only a small number of states, all of them liberal democracies, are succeeding. Among the authoritarian states, though China is the most advanced in terms of cyber-resilience policy, it faces substantial challenges in that area. Overall, no country is satisfied with its level of cyber security and resilience.

On *global leadership in cyberspace affairs*, most countries are diplomatically active but fall into two broad blocs – those led by the US, and those led by China and Russia. The former bloc tends to argue for the application of existing international law to cyberspace and for the continuation of current 'internet freedoms'; the latter argues for new international treaties that would give states greater control over their sovereign cyberspace ('cyber sovereignty'). The view of the US-led bloc has prevailed so far, but China is making significant efforts to influence the relevant diplomatic processes (one example is a Chinese official having secured the post of secretary-general of the International Telecommunication Union). China has also realised the extent to which US predominance in global cyberspace affairs is underpinned by US technological supremacy. It is therefore contesting that supremacy, for example through the Digital Silk Road component of its Belt and Road Initiative and, in the field of mobile telecommunications, through companies such as Huawei. The states that are particularly vocal diplomatically, whichever bloc they align with, are those that have relatively poor cyber security but face cyber threats that are growing exponentially – India is a prime example. The concept of cyber sovereignty can appear attractive to them, which means the US cannot take for granted its pre-eminence in international cyber diplomacy.

When it comes to *offensive cyber capability*, there are a wide variety of doctrinal approaches and differing degrees of constraint. The US and its closest allies have the most technically sophisticated tools, capable of delivering controlled, surgical effect against critical networks, including as part of high-intensity warfare – but their use of those tools is highly constrained. Russia and China, on the other hand, have greater experience of achieving strategic effect through more extensive use of less technically sophisticated capabilities, delivering cyber-enabled operations for influence, and subversion operations, in the 'grey zone' below

the threshold of armed attack. A similar approach has enabled Iran to punch above its cyber weight. The US doctrinal shift in 2018 under its 'defend forward' initiative is in part designed to redress the balance on such lower-threshold operations by countering them directly on its adversaries' networks. Overall, states have yet to establish a common understanding of what constitutes an irresponsible use of an offensive cyber capability. For this to be achieved, states will need to talk more openly about those capabilities.

It is difficult to judge the impact of moves by states to increase the resourcing of their cyber strategies, partly because measuring human and financial resources is in most cases not straightforward. Nevertheless, it is clear that the investments made by the US, China and Russia, in terms of both personnel and money, outstrip those of the other cyber-capable states. Some of those other states compensate through close alliances, especially with the US. The most mature, sophisticated and effective alliance is the Five Eyes. The authoritarian states have nothing remotely equivalent.

No state has progressed far enough on military transformation to allow its armed forces to claim well-integrated and broadly dispersed cyber capabilities covering the continuum of defence and offence. But based on publicly available information, the US moved earliest and has gone furthest on key fronts such as doctrinal, training and force-structure reform. No other state, except perhaps Israel, has succeeded in dispersing cyber capabilities through its broader force structure to anything like the same extent. While close integration between the cyber capabilities of the armed forces and key intelligence agencies seems to be central to military transformation, there are indications that it can lead to issues with command and control. This is illustrated by the ongoing argument in the US as to whether the head of US Cyber Command should remain dual-hatted as head of the National Security Agency.

After the US made the first moves to develop and acknowledge the role of cyber capabilities in national power in the 1990s, the significant leaps forward in this area have normally been in response to strategic shock. Examples include Iran's reaction to the revelation in 2010 of the US–Israeli Stuxnet attack aimed at impeding its capacity to produce highly enriched uranium; the shock to the US and its allies, after 2011, of the new revelations regarding the extent and effects of commercial espionage by China; the impact on Russia and China of the revelation of Five Eyes capabilities in the Edward Snowden leaks in 2013; and the attempted interference by Russia in electoral processes in the US and some European countries in 2016. The cycle of shock and response, including the diplomatic ructions that go with it, appears to speed up with each passing year. For most countries, we can trace the origins of major cyber-policy changes to such shocks. However, given that no state has yet suffered a cyber catastrophe resulting in significant destruction and loss of life, the average rate of progress in reforming cyber policy is no faster than for major reforms in any other area – it is a process that can take up to a decade to produce meaningful change, and one that can never be said to be complete. A significant impediment for each state is the size of its skilled cyber workforce, with perhaps only Israel having adopted a sufficiently radical approach to upskilling its citizens (notably through its use of military conscription). A lesson from the COVID-19 pandemic that can perhaps be applied to cyber resilience is that states cannot afford to wait for a catastrophe to trigger the required rate of investment.

Relative standing

Given the secrecy that surrounds much of the relevant information, a ranking of the 15 countries in terms of cyber capability, based on the categories in the methodology, cannot be definitive. Nevertheless, it is possible to identify a hierarchy and to place each country in one of the three broad tiers described in the introduction to this report, with the first tier for countries with world-leading strengths across all the categories; the second tier for those with world-leading strengths in some of the categories; and the third tier for those with strengths or potential strengths in some of the categories but significant weaknesses in others. There are also cyber weaknesses among the states in Tier Two, and even in Tier One, but they are minor when compared with the significant weaknesses that consign states to Tier Three.

Only the US is strong enough across all the categories to be placed in the top tier. In the second tier we can

put Australia, Canada, China, France, Israel, Russia and the UK. In the third tier we can put the remaining seven countries: India, Indonesia, Iran, Japan, Malaysia, North Korea and Vietnam. Any attempt at a more granular ranking within the second and third tiers would depend on the weighting given to each category. For example, in the second tier, if a combination of world-class cyber security, world-class cyber intelligence, sophisticated offensive cyber capability and powerful cyber alliances were deemed key, Israel and the UK would probably be top. Alternatively, if the decisive factors were the amount of resources – both human and financial – devoted to cyber, unrestrained operational boldness and day-to-day experience of running cyber-enabled information operations, China and Russia would probably be the leading second-tier states. In the third tier, if core strength in cyber security were the most important criterion, Malaysia would be top; but if operational boldness and experience were key, Iran would lead.

However, it could be argued that strength in the core industries that underpin the future development of cyberspace is the decisive category, given how important those industries are to a country's cyber resilience. If so, with its current trajectory, and providing it addresses its weaknesses in cyber security, China would be best placed to join the US in the first tier. And Japan, in the long term, would be best placed to rise from the third tier to the second.

The report makes a clear judgement about the relative national cyber power of the US and China at present, seeing the former as clearly superior. China may well join the US in the top tier in the future – but for that to happen, it would need to do at least two things. Firstly, it would need to create a cyber-industrial complex on the same scale as that of the US and with many of the same characteristics. This would require a much more productive relationship between university research, industry and government. Secondly, China would need to radically improve educational outcomes in cyber-relevant fields, including basic cyber security. Once these domestic foundations of cyber-power equivalence were in place, China would then face a diplomatic challenge. To be able to wield its cyber power for global effect, it would have to begin to demonstrate an ability to work in alliance with other cyber-capable states.

Balance-of-power considerations

There is a broad consensus in international relations, among both states and political elites, that gains in cyber power, and the application of that power in grey-zone operations, have the potential to upset the broader balance of power between the US and its allies on the one hand, and China and Russia on the other. Beyond that broad consensus, there is not much agreement on how this technological competition can be assessed or measured in power terms, a situation compounded by the frequent emergence of new technologies (such as nano chips, carbon-based chips, cloud architectures, quantum computing, AI, autonomous weapons systems and military robots).

Leading states agree that cyber capability underpins military power and can radically affect decision-making and the control of most military systems and force formations. This report confirms that the traditional notion of balance of power based on geopolitical arrangements is being superseded by the idea of an informational balance of power. The US and China both pursue doctrines of information dominance, which includes attempting to dominate the global production of information technology. The US believes it still has the edge, and indeed China concedes that is the case. Moreover, the old geopolitical realities remain in play, especially given the United States' international alliances (through NATO, and with Australia, Israel, the Gulf Arab states, Japan and South Korea). These alliances retain their geographical importance but now carry a new overlay of cyber partnership.

This report takes the view that US digital-industrial superiority, including through alliance relations, is likely to endure for at least the next ten years. There are two strands to this judgement. The first is that in advanced cyber technologies and their exploitation for economic and military power, the US is still ahead of China. The second is that since 2018, the US and several of its leading allies have agreed to restrict, with differing degrees of severity, China's access to some Western technologies. By doing so, they have endorsed a partial decoupling of the West and China that could potentially impede the latter's ability to develop its own advanced technology. How robustly the US continues this strategy, and how China responds, will dictate the future balance of cyber power.

CYBER CAPABILITIES AND NATIONAL POWER:

A Net Assessment

This report sets out a new methodology for assessing cyber power, and then applies it to 15 states:

- Four members of the Five Eyes intelligence alliance – the United States, the United Kingdom, Canada and Australia
- Three cyber-capable allies of the Five Eyes states – France, Israel and Japan
- Four countries viewed by the Five Eyes and their allies as cyber threats – China, Russia, Iran and North Korea
- Four states at earlier stages in their cyber-power development – India, Indonesia, Malaysia and Vietnam

The methodology is broad and principally qualitative, assessing each state's capabilities in seven different categories. The cyber ecosystem of each state is analysed, including how it intersects with international security, economic competition and military affairs.

On that basis the 15 states are divided into three tiers: Tier One is for states with world-leading strengths across all the categories in the methodology, Tier Two is for those with world-leading strengths in some of the categories, and Tier Three is for those with strengths or potential strengths in some of the categories but significant weaknesses in others.

The conclusion is that only one state currently merits inclusion in Tier One. Seven are placed in Tier Two, and seven in Tier Three.

This report is the first product of a cyber-power project undertaken by the International Institute for Strategic Studies. Assessments of the cyber capabilities of many other states will be published in the coming years.

The International Institute for Strategic Studies (IISS)

The IISS, founded in 1958, is an independent centre for research, information and debate on the problems of conflict, however caused, that have, or potentially have, an important military content.

IISS

The International Institute for Strategic Studies – UK
Arundel House | 6 Temple Place | London | WC2R 2PG | UK
t. +44 (0) 20 7379 7676 **f.** +44 (0) 20 7836 3108 **e.** iiss@iiss.org www.iiss.org

The International Institute for Strategic Studies – Americas
2121 K Street, NW | Suite 600 | Washington, DC 20037 | USA
t. +1 202 659 1490 **f.** +1 202 659 1499 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies – Asia
9 Raffles Place | #49-01 Republic Plaza | Singapore 048619
t. +65 6499 0055 **f.** +65 6499 0059 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Europe
Pariser Platz 6A | 10117 Berlin | Germany
t. +49 30 311 99 300 **e.** iiss-europe@iiss.org

The International Institute for Strategic Studies – Middle East
14th floor, GBCORP Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain
t. +973 1718 1155 **f.** +973 1710 0155 **e.** iiss-middleeast@iiss.org