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.