Assessing military cyber maturity: strategy, institutions and capability

Jason Blessing and Greg Austin

February 2022

IISS
The International Institute
for Strategic Studies

Executive summary

One of the most profound influences on the evolution of a country's military cyber forces and strategies is politics. This paper offers insights into how the governance and organisational factors of domestic politics facilitate or inhibit the dissemination of cyber concepts and capabilities throughout military forces beyond the main signals or cyber intelligence agency.

There are at least three reasons to analyse military cyber maturity. The countries currently pursuing such capabilities are not satisfied with the development levels in policy and strategy they have so far reached. There is increasing potential for crippling cyber attacks on key elements of military capability or supporting infrastructure. And no country has yet succeeded in the broad dissemination of cyber capabilities through its armed forces in ways that leading military planners would like.

Few governments have reached an enduring consensus on just how quickly and how deeply reforms in the armed forces must be made to satisfy national security needs. While consensus points have been reached, these are usually tested within a short period of time by international circumstances and technological trends. The main dilemma is whether military cyber strategies and capabilities need more than routine development as just one more element of military power, akin to artillery or submarines; or whether they are sufficiently transformative of military power to warrant radical development pathways and a higher priority than others.

This paper provides an impact matrix which can be used by governments, their armed forces and research analysts to understand the ways in which military cyber reforms can be facilitated or inhibited by governance and organisational processes.

We identify three types of military cyber maturity: strategic, institutional and capability. Within each, we look at four governance factors: senior political-leadership receptivity to military cyber reform; civilian-military relations as they relate to cyber operations; broader 'military modernisation' efforts; and the role of alliances and international partnerships. For each type of maturity, we also assess three organisational influences: competing cultures (within the military and between the military and intelligence agencies); the military's capacity for adaptation; and operational experiences in the cyber domain.

Reliance in the paper on these categories of analysis is a very clear statement of our view that these factors matter most for countries aspiring to mature military cyber capability. Robust governance and high-quality organisation are essential underpinnings of effective and sustainable cyber military operations. Governments which do not manage these considerations as effectively as their peers run a serious risk of being less capable actors in military uses of cyber technologies.

In this process of transformation of a country's armed forces for wide-ranging and sustained cyber operations, 'champions for change' are key (if oft-ignored) catalysts for maturation. These champions are entrepreneurial individuals who make concerted efforts to effectively shape outcomes under the influence of challenging and diverse organisational, governance and geopolitical factors.

The impact matrix is an analytical tool that assists in understanding how influences and choices that are internal to one government and largely under its control might develop. A more comprehensive analysis might also include influences that are external to government reform processes or less tractable to political decision-making. Moreover, the matrix outlines 21 separate influences and by itself could not fully capture the interactions that happen in practice between them. Without trying to document such interactions, the report offers for reflection six brief illustrations of how some of these internal processes interact with each other or with external factors that fall less easily under government control. These vignettes look in order at the United States, China, Australia, Estonia, the United Kingdom and Israel. Each vignette is quite different in style and approach, but provides insight into the confluence of selected factors across different political and military contexts.

Contents

Introduction

As part of a long-term project on cyber power and cyber military capabilities, the International Institute for Strategic Studies (IISS) published in 2021 a methodology for assessing national cyber power which it tested in 15 country studies that included a net assessment of their cyber power.[1,2] Ten additional country studies will be published in the coming months. Based on that work, we conclude that there are three compelling reasons to analyse military cyber maturity. Firstly, countries intent on developing operational cyber capabilities throughout their armed forces that are independent of their central, national-level cyber/signals intelligence agencies are not satisfied with the maturity levels they have reached so far. Secondly, cyber threats to military capability and supporting infrastructure continue to proliferate. Finally, no country has yet found the right balance between the political weight of its central, national level cyber intelligence agency in setting cyber policy and the urgent need to disseminate cyber capabilities, especially for defence, through its armed forces.

Several frameworks exist for assessing cyber security or cyber military capabilities, but none give adequate attention to the main determinant of military cyber maturity – that is, politics, broadly defined. The 2021 IISS study mentioned above shows that this element of national life gives shape to outcomes in national power and cyber capabilities.[3] All major military reforms thrive or founder in the cut and thrust of national politics.

This paper provides a structured approach to better account for the role politics plays through a new cyber military maturity impact matrix. This matrix bears resemblance to maturity matrices used in other disciplines and areas of policy studies and can be understood in a similar fashion.[4] We conceptualise cyber military maturity along three primary dimensions: strategic maturity, institutional maturity and the maturity of capabilities (both offensive and defensive). Geostrategic conditions are certainly an important backdrop for each country; however, geostrategic pressures do not fully account for how and why cyber forces develop in divergent ways that are unique to each country. We thus present a pathway for analysing these political influences. Our approach to the politics of cyber military maturity identifies four governance factors and three organisational influences that shape force-structure outcomes. In considering how these factors interact, this report also addresses a key (if oft-ignored) catalyst for maturation: the role of 'champions for change,' i.e., entrepreneurial individuals who are prepared to build and spend political capital to effectively shape outcomes under the influence of challenging and diverse governance and organisational factors set against a specific geopolitical background.[5]

There is no 'one-size-fits-all' approach to developing cyber military power and highly capable cyber forces. As such, the framework advanced in this paper is a useful tool for governments and analysts evaluating or refining policy processes related to military cyber maturity. No one committed to the acquisition of cyber military power and capability can ignore the politics of achieving this.

This paper does not try to rank or score levels of maturity, nor does it attempt to answer the question of how many cyber personnel a country may need, or how to train or organise them, now or in the future. It does not provide general propositions about how a country should shape its military cyber strategies. Instead, our framework requires those who use it to exercise judgement about the dynamics that facilitate or hinder progress towards military cyber goals and objectives given their respective contexts. What barriers are there to reaching greater maturity? What political currents can be harnessed to advance military cyber initiatives? The matrix exposes these types of questions to provide policymakers with a richer and more nuanced understanding about the likely success or failure of cyber military reform efforts. The matrix provides a framework for a structured evaluation of the prospects for greater cyber military maturity.

The dynamics surveyed in this paper do not occur in a vacuum. They are contingent on each other and are also influenced by external conditions. For that reason,

after presenting a summary of the impact matrix in the body of the paper, and leaving a fuller elaboration of it to the Appendix, we give some illustrations of the factors that have interacted contingently in the case of six particular countries which in order are: the United States, China, Australia, Estonia, the United Kingdom and Israel. These illustrations are just that, and should not be seen as comprehensive case studies. They reveal considerable potential for further research. Three of these illustrative examples (US, China and Australia) take a broader sweep of policy cutting across all three types of maturity, while the following three (Estonia, the UK and Israel) take a much narrower focus, looking mainly at one type of maturity.

Military cyber maturity: a framework

Military cyber capabilities are relatively new to most countries, with little common understanding between governments, military leaders and academic specialists. As with traditional capabilities, the development of a country's military cyber capability represents the confluence of complex and profound choices about the trade-offs of different elements of military power and states of military readiness. Such choices account for geopolitical positioning as well as domestic considerations, from internal security through financial resources, education policy and national industry policy. The question of how many submarines, armed drones or missiles a country needs is almost impossible to answer in any absolute terms. Answers arise in practice from political compromises between different arms of government and the armed forces, and adjustments in governance and in organisations as currents of strategic thought emerge and fade.

Decisions regarding strategic policy, military force structure development and operational use of capabilities should not be assumed to be rational. In some circumstances, analysts may be able to trace a degree of coherence and rationality in capability development and use. Yet, as so convincingly demonstrated in modern political science, and over centuries of military history, institutional and individual biases of commanders, political leaders and the rank and file are more likely to have the upper hand over more rational motivations and processes.[6,7]

In what ways, therefore, can it be meaningful to suggest that there might be an ideal force structure or a maturity level for military cyber capabilities to which states can aspire? There is, unsurprisingly, no consensus, and this paper is not relevant for the very large number of states (around 150) which ignore serious exploration of cyber military capabilities, often by conscious decision but more often because of competing national priorities. Instead of laying out ideal-typical end states for military cyber capabilities, this paper addresses the main factors that will shape the capability available to political and military leaders and ultimately its political utility. Drawing on the authors' own substantial research on national cyber capabilities and military force structure and operations, this paper identifies key considerations that policymakers, in government or the armed forces, should take into account when making choices about the intent and pace of development of cyber military forces.

In some respects, we are setting a single maturity standard for all countries, regardless of size, wealth, threat environment and strategic disposition. Yet our analysis allows for what we might call 'relative cyber maturity'. To explain this distinction, we can compare and contrast two hypothetical aims for military cyber maturity by linking each to a type of country.

Firstly, we can consider a wealthy country, such as the United States, with highly advanced ICT capabilities, a large population, large military forces and global strategic interests. Such a country might plan for cyber options in all phases of military operations in wartime, with wide geographic scope: multitheatre, multivector, multiwave attacks closely coordinated with several war objectives and other military operations.[8] The US might contemplate several types of cyber missions, including:

- cyber defence, especially through deception or denial
- espionage (intelligence collection including acquisition of adversary war plans and weapons designs)
- deterrence
- achieving operational advantage in cyberspace
- supporting theatre and tactical kinetic campaigns to shape the battlefield's information environment
- cyber-enabled information operations (disinformation)
- cyber degradation or destruction
- information corruption
- cyber-enabled psychological operations

In such a case, it would seem appropriate to judge the cyber military maturity of the US based on both its stated objectives and on its potential to execute (or at least to have seriously considered) all of these missions.

We can compare these cyber military-maturity expectations with that of a much smaller country, such as Estonia. The GDP of the US in 2020 was 7,000 times greater than Estonia's. The Baltic country has a population of around 1.3 million, a number smaller than the number of US active military personnel in 2021 (1.388m). The US has at least three times as many ICT professionals as Estonia has people. Estonia's most significant potential military adversary, Russia, has almost as many active-duty military personnel (1m) as Estonia's entire population. Russia also has more ICT professionals than Estonia's entire population. What could cyber military maturity possibly mean for Estonia?

We do not seek to contrast the US and Estonia in these terms. This paper instead focuses on understanding and advancing judgements about policy processes that may be generalisable across states, rather than assessing relative military cyber power. That said, the process of policy deliberation for states' military cyber postures and capabilities must, to be credible, account for national resources, interstate power balances and adversary capability. There has to be some matching of ambition to potential cyber military capability, rather than simply settling for a tokenistic cyber command not backed by appropriate strategies or budget commitments. This may involve considerations about alliance relationships, diplomatic strategies or developmental choices. Thus, we assert that all states need to have at least considered many of the same basic questions, while recognising that only a handful of states are in a position to consider the more complex aspects of cyber military capability.

Conceptualising Military Cyber Maturity

We define maturity as a state's adherence to pathways for establishing highly effective military cyber forces and postures appropriate to its strategic circumstances. The pathways will always be country-specific. As such, this paper provides reflections on how best to assess the pathways of digital transformation that seek to equip a country's armed forces for cyber-enabled operations in war, lower-intensity conflict or deterrence, given that state's particular strategic setting. In many respects, military developments for cyberspace are no different from other types of military reforms.

The paper's focus on military cyber transformations is intended to emphasise changes outside any pre-existing arrangements with civilian cyber or signals intelligence organisations. For example, the paper is not interested in long-established national-level agencies, such as the National Security Agency (NSA). Instead, it is more concerned with understanding the establishment pathways of new military organisations, such as the United States Cyber Command or new cyber units in operational commands like those now being established in the US Space Force. Of course, there is an unbreakable symbiotic link between any military cyber operations and primary intelligence agencies such as the NSA (which is in any case subordinated to the Secretary of Defense). Cyber effects of military significance, either on the battlefield or on battle management systems, can be delivered by an intelligence agency without the need for independent military cyber units. It is also true that leading states, such as the US, the United Kingdom and Australia, have favoured military cyber reforms that leave the traditional cyber/signals intelligence agency with a leading role in new military cyber policy, operations and institutional reform. Thus, the paper's primary focus on reform pathways outside of the main national cyber/signals intelligence agency may appear inappropriately narrow and somewhat artificial.

However, there are at least three strong arguments in favour of our approach. Firstly, a centralised cyber/signals intelligence agencies cannot possibly defend the thousands of unique computer systems in a country's armed forces. Secondly, many states have the ambition to exploit offensive cyber operations in localised situations in the context of tactical or even theatre-level events for which a centralised agency would likely be ill-equipped to monitor or control. Thirdly, as the leading cyber powers increasingly look to conduct high-intensity combat operations involving advanced cyber operations on a large scale, this new circumstance may place such national and non-military demands on the leading cyber/signals intelligence agency so that its ability to prioritise military combat operations would likely be reduced.

The paper's focus on reforms outside of partnerships with the main cyber/signals intelligence organisation may still appear questionable in a situation where some states, such as the UK, have staked much on a hybrid solution for force structure development. In what is a unique pathway, the UK has decided not to create a military cyber command, but rather an organisation involving military and civilian assets combined under dual reporting lines to ministers.

By 'military cyber' we therefore mean all of those cyber-enabled operations undertaken by units and organisational elements under the control of uniformed officers in formal military structures reporting through the military chain of command (although some units may be staffed by both civilian and uniformed personnel). This definition allows for consideration of cyber-enabled operations for military purposes by agencies like the NSA and Government Communications Headquarters.

Technological improvements, strategic and doctrinal innovations and institutional reconfigurations are three universal dimensions along which armed forces can innovate and mature.[9] Maturation in these dimensions is likely to be discontinuous and uneven, and achieving high levels of maturity in each category for a given reform will be quite rare.[10] Aspiring military reformers face many rational and irrational sources of institutional and interpersonal friction. Few are able to connect the elements of change with the required political capital

during domestic and geostrategic windows of opportunity to advance wide-ranging and substantive policy shifts. As in other policy areas, military policy experiences long periods of stasis, with incremental change followed by dramatic and punctuated change within a short timeframe. Breakthrough inflection points introduce and crystallise new paradigms, after which incrementalism and 'muddling through' the policy process resumes.[11]

Thus, while recognising these dynamics, we conceptualise cyber military maturity along three primary dimensions: strategic maturity, institutional maturity, and the maturity of capabilities (both offensive and defensive). These aspects can certainly overlap, and developments along one dimension will inevitably impact developments in others. Yet, disaggregating maturity according to these three dimensions allows for important insights into how governance and organisational factors can influence the development of military cyber forces in different ways. Box 1 provides short definitions for these three dimensions that are discussed in more detail below.

Box 1. **Three Dimensions of Military Cyber Maturity**

Strategic Maturity: The degree to which military organisations and their leaders have devised concrete plans to develop and utilise cyber capabilities in support of national security goals in key theatres of operations and have demonstrated the political leadership to implement the declared developmental and operational goals.

Institutional Maturity: The degree of effectiveness with which a military organisation has harmonised its planning, force preparedness and execution to deliver cyber operations in support of national security goals in key theatres of operations.

Capability Maturity: The extent to which cyber forces have developed defensive and offensive cyber options and the level of human skill required to utilise them in key theatres of operations in line with strategic intent and organisational demands.

Strategic maturity refers to the degree to which military organisations and their leaders have laid out concrete plans to develop and utilise cyber capabilities in support of national-level security goals in key theatres of operations and have demonstrated the political leadership to implement the declared developmental and operational goals. Plans for developing and utilising cyber capabilities can encompass the use of cyber capabilities independently of traditional kinetic operations, the integration of cyber capabilities into traditional operations and the use of cyber tools to enable other types of operations, such as psychological or information operations. More broadly, strategic maturity can be reflected in documents that lay out organisational or policy priorities and budgets. As such, military organisations displaying high degrees of cyber strategic maturity are likely to have clear budgetary and policy priorities, well-developed frameworks for using cyber capabilities in a variety of operational settings, and a broader vision of how military cyber operations relate to other forms of strategic military action.

Doctrinal developments surrounding the use of offensive cyber capabilities would be a more powerful marker of strategic maturity. For example, military organisations which view cyber operations simply as a way to ensure continuity of information and communications technologies exhibit lower levels of strategic maturity than those seeking to gain information superiority and produce independent military effects in cyberspace.

Use of the word 'strategic' in a military planning context often evokes a question about the operational and tactical levels of war. It is a common assertion that cyber capabilities can flatten the once-strong hierarchy of strategic–operational–tactical. Accepting that this may occur under certain conditions, this paper proposes that it is possible to differentiate strategic maturity from tactical or operational maturity. Tactical maturity might encompass frameworks for the proximate and frequent use of cyber capabilities by a small number of operators that can keep effects somewhat localised, producing only tactical outcomes.[12] At the operational level of warfare, maturity might be conceived around the development of concrete concepts of operation seeking effects for theatre-level outcomes, or the outcomes of

large campaigns. In contrast, strategic maturity refers to the use of cyber operations at scale and with greater scope, reach and effect at the level of war outcomes. In a maximalist sense, this means that cyber capabilities are used (independently or in conjunction with kinetic operations) to form multitheatre, multivector, multiwave attacks that can produce effects that reach past an adversary's military formations and into the strategic choices of its political leaders about how to fight the war or whether to abandon it.

Institutional maturity reflects how effectively a military organisation has harmonised its planning, force preparedness, and execution to deliver cyber operations in support of national-level security goals in key theatres of operations.

The degree of interplay between civilian and military leaders, as well as the overall responsiveness of institutions in relation to the cyber mission, sheds light on this important dimension of maturity. The degree to which non-cyber military organisations accept and embrace the cyber mission also provides a particularly powerful insight into the institutional maturity of cyber forces. Assessments of institutional maturity can encompass several other potential indicators. Within the military ecosystem, these might include: how well positioned a cyber force is to secure funding vis-à-vis other military organisations; the extent to which training and personnel career tracks have been standardised; the formalisation of inter-organisational relations; and the degree of operational independence. Just as important is the maturation of bureaucratic ties between military cyber forces and their civilian intelligence-agency counterparts. Military cyber forces with higher levels of maturity are more likely to have developed formal mechanisms for deconflicting and/or coordinating cyber operations conducted by civilian intelligence elements.

Capability maturity indicates the extent to which cyber forces have developed defensive and offensive cyber tools and the levels of human skill required for utilising them in a manner corresponding to strategic intent and the organisational demands.

A robust cyber-intelligence capability (i.e., 'cyber-espionage' capability) is certainly a key underlying condition for the maturation of cyber capabilities, as is the broader civilian digital economy upon which many capabilities rely. However, a crucial dimension of capability maturity is moving from the ability to gather intelligence on computers and networks to the ability to deliver effects that disrupt, deny, degrade or destroy networks and/or computers. Deception in cyberspace (cloaking cyber intrusions, creating false impression of the purpose of an attack and setting up 'honey pot' systems) is also an important indicator of capabilities maturity. While operational experiences could provide critical indications of capability maturity after the fact, much information may remain highly classified. The armed forces of some countries may not even conduct offensive operations. In these cases, military exercises can provide some insight into a cyber force's capabilities. Those forces that are able to stage domestic exercises are likely to maintain higher levels than cyber forces that do not. The purposes of exercises – such as whether a 'red-teaming' dimension is included – can also be reflective of capability maturity.

The impact matrix in brief

We have chosen the concept of an 'impact matrix' as a means for enabling governments, military leaders and analysts to quickly grasp both the big picture of military cyber maturity and the many underlying factors. The matrix is presented in Figures 1 and 2. For the sake of simplicity, this initial graphic presentation is two- dimensional.

For each type of maturity (strategic, institutional, capabilities), we analyse two sets of factors: governance and organisational. The order in which factors are presented below functions as an outline for our discussion and does not reflect their relative importance in the matrix. A full discussion of each of these factors across the three dimensions of maturity can be found in the Appendix.

Under governance, we look at:

- senior political leadership's receptivity to military cyber reforms
- civilian–military relations related to cyber operations
- broader 'military modernisation' efforts
- the role of alliances and international partnerships

Under organisational factors, we look at:

- operational experiences in the cyber domain
- the military's capacity for adaptation
- divergent cultures (within the military and between the military and intelligence agencies)

Table 1 and Table 2 below bring these factors into graphic form in a simple matrix. Each cell offers an illustration of the potential impact of variations in the particular combination of a named "factor" and the type of maturity.

The impact matrix might in a scientific sense be more reliably represented as multi-layered and multi-dimensional to better capture the interplay between the different types of maturity and the various factors. A multi-dimensional matrix would certainly be essential to understand the impact on the factors named in the matrix of other profoundly influential factors not yet mentioned, such as the impact of time, the availability of funding, and workforce availability.

Table 1: **Governance Factors in the Military Cyber Maturity Impact Matrix**

Governance Factors	Strategic Maturity	Institutional Maturity	Capabilities Maturity
Senior political leadership receptivity	• Interest in cyber options can *facilitate*. Turnover can result in new champions. • Sceptics can *inhibit*. Turnover can disrupt maturation.	• Support and leadership continuity can *facilitate*. • Obstruction and turnover can *inhibit* and delay progress.	• Continuity and long-term vision can *facilitate*. • Unwillingness to devote political capital and turnover can *inhibit*.
Civil–military relations on cyber operations	• Reconciling military and civilian intelligence imperatives can *facilitate*. • Prioritising military or civilian intelligence over the other can *inhibit*.	• Defining productive military–civilian intelligence relationships can *facilitate*. • Military–civilian intelligence bureaucratic rivalry can *inhibit*.	• Managing interdependence of military and civilian intelligence capabilities can *facilitate*. • Prioritisation and military or civilian capability guarding can *inhibit*.
Military modernisation	• Late reform stages can *facilitate*. • Early reform stages can *inhibit*.	• Consolidation and redefinition of hierarchies can *facilitate*.	• Later stages can *facilitate*. • Early stages can *inhibit*.
Alliances	• Information sharing and certain political frictions can *facilitate*. Varied development can limit utility of information.	• Consultations and interoperability standards can *facilitate*.	• Exchange of 'best practices' among operators can *facilitate*. • Unwillingness to share technical tools can *inhibit*.

Table 2: **Organisational Factors in the Military Cyber Maturity Impact Matrix**

Organisational Factors	Strategic Maturity	Institutional Maturity	Capabilities Maturity
Operational experiences	• Field testing can *facilitate*. • Pre-existing biases and uncertain signalling dynamics can *inhibit*.	• 'Proof of concept' can *facilitate* bureaucratic expansion.	• Exposure and operational feedback can *facilitate*.
Military adaptive capacity	• High levels of adaptive elements can *facilitate*. • High redundancy can *inhibit* by increasing veto players.	• High complexity, loose coupling and low redundancy can *facilitate*. • Low complexity, low experimentation and high redundancy can *inhibit*.	• High levels of adaptive capacity can *facilitate* in early maturity stages. • High redundancy and loose coupling can *inhibit* in later maturity stages.
Divergent cultures	• Reconciling subcultures via cross-domain frameworks can *facilitate*. • Subcultural clashes, overexploitation and disruption can *inhibit*.	• Common frames for the cyber mission can *facilitate*. • Competition over the cyber mission and over-classification can *inhibit*.	• Perceptions of 'cultural fit' can *inhibit*.

Analytical Challenges

This study engages with many fields of political and social science, strategic studies and contemporary history. At the same time, it makes judgements about how countries assess and manage their optimal force structures. It seeks to form a view of the historical trends that have shaped force-structure outcomes over the past two decades, a process that highlights the risks and shortcomings of writing history of bureaucratic politics in the very recent past.

Overlaying these considerations is a question fundamental to the entire exercise: has the information age created the opportunity for a revolution in military affairs? Some countries act as if the answer is yes. The question itself is highly political and highly consequential for transformations in the armed forces of numerous countries. However, many see little value in the in-principle acceptance of a cyber revolution in military affairs when it comes to determining what type and degree of cyber capability are enough. We are also still at the dawn of the cyber age, and this means that the horizons of cyber military maturity may keep receding as military reform progresses.

Given that many aspects of military cyber reform and capability remain hidden from the public eye, the study is forced to make conclusions where some evidence remains thin. Nevertheless, it draws on research by the authors in their doctoral studies and in connection with their work on country studies and military data collection for the cyber-power project of the International Institute for Strategic Studies. We thus have high confidence that the sorts of considerations we raise and our judgements on key issues still serve as useful reference points for the intended purposes.

There are two additional factors that complicate the analysis at hand: ambition and time. Does a country desire to be a pre-eminent cyber power? Or is the goal to develop a baseline defensive posture? The global or local vision for one's military is certainly an important enabling (or constricting) condition for cyber military maturity, but ambition can also relate to the desired degree of military change at the domestic level. Do military reformers seek to graft the cyber mission onto existing organisations and procedures, or do they want to completely disrupt and transform the military by institutionalising 'new ways of war'?, Ambition provides the guardrails for future maturation, but ambition and visions for cyber military maturity may not match what is feasible in terms of political conditions.[13] Disentangling varying levels of ambition among actors and its feasibility is far beyond the scope of this report, but we acknowledge that the dynamic underlies many of our judgements.

The passage of time carries its own implication for our analysis. On the one hand, there are temporal dynamics at the international level to consider. There is certainly a first-mover advantage in the development of cyber capabilities. Yet, that advantage decreases with the passage of time, as more states develop their own military cyber forces and the maturation costs for laggards continuously decline.[14] On the other hand, the timing and sequencing of military change efforts can impact reform momentum and eventual success or failure.[15] Importantly, the passage of time provides crucial space for maturation to take place, but it can also provide space for regression and lost momentum.

Considering these analytical challenges, the case studies below stand as important explorations and illustrations of the dynamics portrayed in the cyber military maturity impact matrix. They are by no means comprehensive; instead, we intend to use empirical evidence from each case to show the different ways in which maturity can unfold – whether across specific dimensions or as a whole.

Champions for Change

The preceding judgements have considered the effects of governance and military-organisational factors; however, the role of individuals cannot be overstated. It is individuals who ultimately make and implement policy. With respect to military cyber forces, entrepreneurial individuals – champions for change – are crucial to the convergence of factors shaping strategic, institutional and capability maturity.

Successful cyber-force champions can play both advocacy and brokerage roles in the course of military innovation and implementation. In carrying out these roles, they can bring a variety of traits that facilitate efforts to achieve higher levels of maturity to the table. Firstly, such individuals can (but do not need to) occupy decision-making positions where they hold the necessary authority and resources to overcome bureaucratic hurdles. Secondly, they can possess important negotiation skills that build connections with stakeholders and cultivate interpersonal trust. Thirdly, champions could also possess technical expertise that confers a degree of authority or credibility in driving through reform measures that match the expertise. Additionally, successful entrepreneurs can have extensive career experience spanning civilian and/or military bureaucracies. Finally, champions are persistent but patient for windows of opportunity.

For strategic maturity, one of the most important functions of cyber champions is to connect the utility of military cyber operations to the geostrategic concerns and bureaucratic interests of others. When these individuals do not occupy leadership positions, briefings and inter-agency meetings present likely forums for obtaining buy-in from senior leaders and other stakeholders. When coupled with career experience, playing this translating role is a crucial part of overcoming the institutional and cultural barriers that can exist between cyber forces, civilian intelligence agencies and other military commands. In particular, champions can aid the development of frameworks or inter-agency processes to assess and mitigate the potential intelligence losses from military cyber operations. Within the military, successful entrepreneurs are able to define the cyber mission both independently and in relation to existing military engagements. Importantly, they can enlighten conventional commanders as to what cyber capabilities can and cannot do for them. Doing so can promote strategic maturity by ensuring that cyber capabilities are not developed and deployed in isolation from conventional military means.

Champions can play an outsized role in the pursuit of greater institutional maturity, particularly when those efforts entail the creation of a new organisation. Interpersonal trust and expertise are critical resources for undertaking wide-ranging reforms that benefit cyber forces. Champions with a range of personal connections across the defence ecosystem have the potential to bring stakeholders – many of whom may not be aware of each other – into a single room to discuss organisational reforms. Individuals can also leverage their expertise and others' trust to gain buy-in for institutional initiatives. For example, military commanders who have neither the know-how nor the capabilities for the cyber mission are more willing to support initiatives from a 'champion' they know and trust than from someone they do not. When civilians and other military commands have a vested interest in conducting cyber operations, interpersonal trust helps to lower the costs of coalition-building in support of greater institutional maturity.

Finally, champions can facilitate capability maturity at both the technical and political levels. At the technical level, entrepreneurs can recommend the use or acquisition of new tools or the application of existing tools in new contexts. At the political level, champions can be the primary advocates for capability and personnel investments. They can also serve as important points of contact for coordinating capability development across stakeholders to reduce duplicated efforts. As a coordinator, their ability to act as translator between technical and policy-oriented communities helps ensure that capabilities are matched to mission needs.

Maturity challenges: selected examples

To illustrate the confluence of the governance and organisational factors across strategic, institutional and capability maturity, we present selected examples of maturity challenges from the experience of five countries: the United States, China, Australia, Estonia, the United Kingdom and Israel. In each of these short examples, our judgements focus on some of the forces that drive and/or hinder a military's cyber maturity. Each example also highlights the contingent nature of the maturation process.

While no country is fully mature, we assert that the US has achieved greater overall military cyber maturity than any other country. China represents a more middling case of maturity, with progress in some aspects and less visible progress in others. Finally, Australia's armed forces provide a case full of potential where maturity efforts were stunted by several political dynamics until being unleashed progressively after 2016. Yet they remain very much a work in progress with horizons for reform now stretching into the next decade. Estonia is an example of a small state that has effectively put political resources and means to strategic ends and is thus relatively strategically mature. The UK provides a case of institutional maturity that rests on navigating operational feedback, resource constraints and new civilian-military dynamics. The Israel case, through its relatively advanced capability maturity, shows the importance of both operational experience as a testing ground and of a strong relationship between military cyber forces and a broad and innovative ecosystem.

For brevity's sake, the discussion of these example represents an assessment and not a detailed evaluation against each of the nine sub-elements in the matrix under each of the three types – since that would be 27 separate discussions.

Our assessment is values-based, but the values we apply are not those that reveal a preference for one political system over another, or moral norms that privilege state surveillance over the privacy of citizens, but rather a preference for those strategies that maximise the application of strategic power through leveraging military cyber assets. That said, the strategic power of a state is often underpinned by its moral authority and its political standing among other states – also known as 'soft power'. This is particularly relevant in assessing the fourth governance factor: the role of alliances and international partnerships.

For each of the illustrative studies presented in this report, we base our judgements on research undertaken for completed country studies in our cyber power project, which includes the 2021 publication, 'Cyber Capabilities and National Power: A Net Assessment'. We also rely on a variety of 'leading indicators' based on parallel efforts at the the International Institute for Strategic Studies (IISS) to collect and assess cyber-focused data for *The Military Balance* book and the associated database, The Military Balance+. These indicators include:

- principal cyber forces and other leading organisations
- military roles
- national strategic documents (national, defence, and military)
- national command and control arrangements
- offensive cyber operations

Selected Lessons from the US

The US is farther down the path of military cyber maturity than any other country. Beginning in the 1960s, it has amassed high level ICT capabilities in all categories of cyber power that contribute to its current military cyber power. From that time on, the armed forces began to institute wide-ranging organisational and doctrinal measures for military cyber power. They adjusted their recruitment, training and military exercises accordingly. Through this decade, building off experience in the 1991 Gulf War, US combat forces came to rely increasingly on advanced cyber military capabilities. In 2021, IISS judged the US to be the only country with world leading strengths in all of those aspects of cyber power. At the same time, when it comes to the military dimension of that cyber power, there is clear evidence, unsurprisingly, that the

development pathway has not been entirely smooth. The US certainly has several highly mature elements in its military cyber posture, and its military leaders already stake much on use of such capability in war. Yet, political and military leaders believe it has fallen short of optimal military outcomes that match its full potential in this field or the military threat from other countries. The US is not satisfied with its current levels of military cyber maturity.

Operational Experiences in the Cyber Domain

In military reform, there may be nothing more powerful in driving change than operational experience as proof of the value of a new technology and its uses.[16] Such experience is one of seven key elements in our maturity matrix. The US has significant operational experience in all areas of military cyber activities that are important to it: cryptology; information security and assurance; cyber-enabled weapons use for targeting; espionage; active defence and counter-espionage; cyber sabotage; and cyber-influence operations. The US most likely has the highest level of maturity across this set of cyber activities (operational military experience) compared to any other country.[17]

For example, as early as 1965, US armed forces were developing computer-assisted targeting and guidance systems.[18] US military espionage in cyberspace most likely began as civilian and military uses of ICT by adversaries and other targets of interest became more common through the 1960s, including the DARPA network project, a defence undertaking that subsequently became the Internet.[19,20] The need for cyber defence was recognised by the Pentagon as early as 1972. US sabotage operations in cyberspace began later. The start date for cyber sabotage planning by the armed forces might have been in the late 1980s, since the CIA began its first course on covert cyber operations in 1990. The significance of US use of cyber-based tools for a range of missions in the First Gulf War in 1991 is debated, but the world took notice of both the precision-strike capability enabled by computer systems (including computerised processes for intelligence collection and geo-location) and the information systems that monitored the attacks from the air or outer space and transmitted them at the speed of light to a variety of US military and government locations around the world. There are reliable reports that in 1999, the US armed forces used cyber sabotage in wartime for the first time against the Belgrade electric grid in the short war against Yugoslavia. US Air Force cyber units were deployed to the conflict.

Military cyber units of the US armed forces outside of the National Security Agency (NSA) have been accumulating operational experience since the mid-1990s, even as they have been expanded and transformed enormously. For example, in 1998, the US Army tasked its 704th Military Intelligence Brigade to develop a 'computer network operations force' for the service. The formal establishment of Cyber Command in 2010 was a boost to the non-NSA cyber operations by US military personnel even though Cyber Command remained closely tethered to NSA through the dual command structure where one person led both organisations, as well the Central Security Service (the national and military cryptology service). By 2018, the US defence system counted 238,000 personnel dedicated to cyber-related duties.[21] These military and defence personnel resources are complemented by those available in the private sector which is regularly contracted for military cyber missions across almost all functions. This is based in part on the access of all relevant military agencies, such as Cyber Command, to research and development (R&D) and special project funds. The budget request for FY22 for defence information technology and cyberspace was US$50.6 billion, of which US$5.5bn was for cybersecurity, US$4.3bn for cyberspace operations and US$510.9 million in R&D funding, in addition to the US$605m for US Cyber Command's general budget.[22]

Because these institutions have been operating and expanding for a significant length of time, we can begin to form a very rough estimate of the number of person years of planning and execution of military cyber missions. We can also overlay that with some sense of the many and diverse combat and peacetime activities that these units have been involved in – Africa, Asia, Europe, Afghanistan, Iraq, Yemen and Yugoslavia.

The geographic footprint of US military cyber operations is global, supported as they are by the US fleet of satellites and other communication devices, as well as by intelligence platforms in motion (on land, on or under the sea, and in the air). The scale of the information-processing assets possessed by the US, used to integrate the data

collected from these operations or to help execute them, is unequalled by any other country. America's ability to maintain this global footprint in 2021 is based on a very large network of allied intelligence agencies (for example, the Five Eyes network, NATO allies, and close security allies, such as Israel, Japan and South Korea), and partnership arrangements with certain countries less politically close but cooperating on cyber operations of one kind or another.

The reach of such operations can be deep. For example, US military cyber agencies have penetrated some of the most sensitive targets and executed cyber-sabotage operations in certain countries, such as the Stuxnet attack (campaign) on the Natanz nuclear-enrichment facility in Iran beginning in 2007 or 2008 and, reportedly, the attacks beginning in 2013 on control systems of North Korean missiles in flight or just prior to launch. The level of technical sophistication of some cyber military operations has been very high, with corresponding levels of success. Two examples that stand out are Stuxnet and Flame, developed in conjunction with Israel. The Snowden revelations also demonstrated the reach and deep penetration of US cyber operations.

The current US vision for its military cyber capability is laid out and developed in more public documents than for any other country. Beginning in the late 1990s, the currently approved documents extend to thousands of pages of doctrine and policy statements endorsed by the Joint Chiefs of Staff (JCS), similar single-service documents derivate of the various joint doctrines, and Department of Defense (DoD) statements of cyber military policy.[23] The documents that most effectively capture the sheer audacity of the US ambition are the vision statements by the two heads of Cyber Command, admiral Michael Rogers in 2015 and General Paul Nakasone in 2018.[24] According to Rogers, the US ambition was to provide, in the fullness of time, cyber-attack options in all phases of operations and at every level of command.[25] On the defensive side, the hope was that cyber defences would be wide-ranging, robust and highly resilient. Both goals remain ambitious, but the country is well ahead of any other in offensive capability.[26] Even so, its military preparedness could be severely damaged by a cyber attack in the event of a major war: comprehensive defence in cyberspace is hard to impossible.[27] According to Nakasone, the mission was 'to achieve cyberspace superiority by seizing and maintaining the tactical and operational initiative in cyberspace, culminating in strategic advantage over adversaries'.[28] The same goal is expressed differently in the 2018 document in novel terms of a temporary operational edge 'in all domains', 'in preparation for and during joint operations in conflict, as well as below the threshold of armed conflict'. In 2020, the commander of the US Indo-Pacific Command at the time, admiral Davidson, made one of the most ambitious statements of US military cyber planning in a speech clearly aimed at China and other potential adversaries. He said that the US would use network warfare to achieve 'penetration and then disintegration of an adversary's systems and decision-making, thereby defeating their offensive capabilities'.[29] It should be noted that many officers in the US armed forces and many scholars are quite sceptical of the sort of ambition expressed by Davidson: that the US could use cyber attacks to paralyse decision-making in China to the extent that the net effect would be to significantly blunt the delivery of their kinetic capabilities. No other country has published such ambitious claims about its cyber capabilities or offered such detailed elaboration of its military cyber ambitions.

In these decades, the US has consistently adopted a variety of policies premised on its military technological superiority over actual or potential adversaries. This view was one element of an ambition for global power matched by few countries since then, such as China, France, the UK and the USSR. Of these, only China still aspires to sustained global influence and to what it sees as the associated military industrial power that must be developed to underpin such global influence. This central aspect of US military policy (the ambition for global preeminence and the leading position in all military-related technologies, including new or emerging technologies), gives any ambition held by the US armed forces for military cyber capability a political authority and weight in domestic politics and international affairs that is simply not currently matched by any other country, with China as a possible exception. From the earliest days of US military interest in strategies of information warfare in the 1990s, these ambitions and visions have been under development, gaining support at the Joint Chiefs level and seeing reflection in budget decisions and, more recently, in operational decisions.

Divergent cultures

Who in the armed forces leadership shares this ambition and vision and how deeply do they identify with them? We can identify clear champions of policy change in favour of the cyber transformation since the mid-1990s, when admiral Bill Owens was the vice-chairman of the JCS Admiral Owens joined with Professor Joseph Nye in 1996 to publicly advocate for US exploitation of its information edge.[30] Since that time, the Joint Chiefs and successive administrations have supported the growth and entrenchment of cyber capabilities in the armed forces. However important such a general commitment has been, the operational significance for future combat of past experience and potential use for offensive purposes is far from settled. The operational experience outline above, especially for offensive cyber operations, has rested largely with the centralised agency, NSA, and after 2010 with the combined operations of NSA and Cyber Command.

A RAND study has identified three strands of thought (better thought of as ideological dispositions) in the US defence establishment on cyber operations: '*sprinkleism*' (little bits of information operations are acceptable and are usually an afterthought); *full commitment to the potential* of information operations through structure, resourcing and integration; and a *paradigm shift to full acceptance of and planning* for outcomes where the information environment is the 'primary determinant of those actions'.[31] The report leaves little doubt of its authors' view that the DoD is stuck somewhere between 'sprinkleism' and full commitment to the potential information operations, and is not yet on the path to the paradigm shift that would be visible in execution of the potential of cyber operations.[32] This view is reflected in the memoir of the former National Security Adviser John Bolton, who commented that the administration had been paralysed 'month after month' in its efforts to be more combative in cyberspace by 'bureaucratic inertia, turf fights, and some genuine unresolved issues'.[33] He was lamenting the 19 months that had passed since Trump's inauguration and the failure of the administration to agree a revised version of legal authorities of offensive cyber operations. Based on more recent indications, senior military officers have reported in private that there has been a fundamental transformation with the DoD over the past seven years in terms of cyber military preparedness and political willingness to use those assets.

There is not a strong consensus in US military culture around potential uses of cyber military capabilities and even the extent to which they should be developed. This is a weakness in the US level of institutional maturity, but based on our analysis of other great powers, the phenomenon of 'sprinkleism' is not confined to the US.

In Congressional hearings for his confirmation as Commander of US Cyber Command in 2018, Nakasone affirmed that the US political leadership would make choices about cyber operations in war based on options that he would present.[34] This is a useful reminder that leadership choices about strategic options, and not the technologies themselves, would determine the scope of transformation towards widespread reliance on cyber operations for coercive purposes. Our analysis suggests that with just a dozen or so exceptions, US offensive cyber campaigns by the armed forces outside of NSA are a quite recent phenomenon. It is notable that their start dates precede the Trump administration and its decision in 2018 to loosen legal authorisation for the approval of offensive cyber operations. Cyber coercive options by the armed forces have not been high in the minds of political and military leaders in any consistent manner between 1999 and 2021.

One possible explanation for this is the way in which the intelligence function in cyberspace has persistently been more prominent for political leaders than the as-yet untested coercive potential of cyber operations – let alone a higher level and more extensive cyber campaign. Another explanation has been the organisational setting in which Cyber Command, the NSA and the CIA have navigated the evolution of the coercive potential of cyberspace. This appears to have constrained a more rapid evolution of cyber coercive operations and campaigns by the armed forces outside of NSA.

Cyber Command has not achieved deterrence in cyberspace yet and nor has it succeeded in integrating 'cyberspace capabilities and forces into plans and operations across all domains'.[35] Its position in peacetime policy circles in the DoD in 2021 is somewhat akin to that of the nuclear-missile submarine fleet in the US, and even the very idea of nuclear propulsion,

in the 1960s and early 1970s. According to a study by the US Navy Historical commission, the 'issue was not whether nuclear propulsion should be developed on a high priority but, rather, whether the potential impact of nuclear power on the Navy warranted more than routine development'.[36] The future of the capability and its uses depended largely on political choices and leadership of competing policy options through intense bureaucratic battles about priorities and funding.

It is certainly ironic that in spite of the still-transitional character of Cyber Command planning and development, its creation, continuing evolution and activities have had a profound impact on strategic affairs globally. Many countries have moved to set up similar commands and/or cite the US move as major turning point in global strategic policy.

While we can conclude that the US has been the leader (or first mover) in the cyberspace arms race, in both intent and capability, we should not discount the inevitability that other countries would move in that direction even if the US had not. A top-secret study on the nuclear-arms race commissioned in 1984 by the US government found that US and Soviet choices were mostly shaped by their technological opportunities and preferences, rather than by what the other state was doing.[37] We should also consider evidence that both Russia and China were at least thinking about the imminence of the change, in part under the influence of US actions, but in larger part because of trends in technology. Examples in history of simultaneous pursuit of a military technology without there being an identifiable first mover (arms-race leader) are numerous.

For this reason alone – technological opportunity – we can expect to see a move away from DoD 'sprinkle-ism' and the eventual paradigm shift foreshadowed by the information dominance advocates. But there is another reason as well. The advent of offensive cyberspace operations, and their potential to displace the physical damage of kinetic weapons, has undermined the pre-existing concepts of the political utility of warfare in and through the information environment. Regardless of the variety of pre-existing dispositions in DoD towards Cyber Command, the global evolution toward malicious activity in cyberspace, especially for military advantage, will almost certainly favour a more decisive move by the Pentagon towards this paradigm shift. That transformation could take a decade more, unless and until there is high-level leadership able to break away from old conceptions of warfighting and victory largely by kinetic means.

There is a contrast between the recognition within the US armed forces and security agencies of this concept of cyber experimentation and the approach of some in the scholarly community in understanding cyber operations as if they were a completed and established phenomenon. The scholarly consensus appears to have arrived at the point where 'none of the degradative cyber operations to date are thought to have been strategically successful'.[38] Yet US military commanders actively plan for that strategic success, based in large part on network warfare. For example, as mentioned above, admiral Davidson made a rare public threat against China of US intent in a war against it: to achieve 'penetration and then disintegration of an adversary's systems and decision-making, thereby defeating their offensive capabilities'.[39] Simply put, it is very firmly the US government's view that what has been made visible in the public domain in terms of offensive cyber capabilities is a mere fragment of the country's warfighting potential in cyberspace. That potential has been accumulated in the twenty years since the US used a cyber attack against the Belgrade electric grid in 1999 to shut it down on at least one occasion.[40] Even when Cyber Command was launched over a decade later, the view was, according to the current commander of Cyber Command, that the US 'had only just begun to understand how cyberspace would become a pivotal forum for great power competition'.[41] He referred to the emergence of new types of missions, including defence of domestic elections from foreign political and technical interference.

Leading Organisations

As noted before, for the purposes of this study of military cyber maturity our definition of 'military' is all of those units and organisational elements under the control of 'uniformed' officers. Some of these units will be staffed jointly by civilian and uniformed personnel.

In the case of the US, the analysis does not include the president, who is the commander-in-chief of the armed forces, nor the secretary of defense, who is part of the chain of command for military operational matters as well as development. Nevertheless, since the governance documents and organisational authority flow from the president and/or secretary of defense, their influence is directly manifested in what the senior military leadership does. The same consideration applies to the role of secretaries responsible for the single services (such as the secretary of the army).

There are three key sets of military or defence actors in the cyber-related developments and operations of the US armed forces:

- the NSA and its sister agency, the Central Security Service, alongside the Central Intelligence Agency and other intelligence organisations
- the chairman and vice chairman of the JCS, and the service chiefs themselves (single service commanders, such as chief of the Air Force)
- Joint Unified Combatant Commands, especially – but not only – Cyber Command[42]

The three corresponding functions, not completely separate from each other, can be understood as:

- intelligence collection
- raising, training and sustaining for the single service chiefs, with the chairman and the vice chairman of the Joint Chiefs playing additional advisory roles for operational matters
- operational matters and warfighting, including covert operations and special operations that can occur in conjunction with the CIA

One of the organisational strengths of the US armed forces when it comes to dissemination of cyber capabilities and cyber options throughout is the existence of well-funded and large single service cyber commands (Army, Navy, Air Force, Marines, and Coast Guard). This also includes the new service, US Space Force, having its own dedicated cyber components. This dissemination goal is also well served by the allocation of Cyber Command's cyber mission teams to other combatant commands, such as Indo-Pacific Command and Europe Command.

These leadership elements, their associated subordinate units, and missions are simultaneously in play in the processes of maturation of policy. The interplay between them is shaped by the preferences and biases of the individuals in the posts and/or those of their massive supporting staffs. The range of opportunities provided by the power of these leaders to shape the development and use of cyber assets by the US armed forces is immense. At the same time, they are constrained or enabled by organisational and structural realities, especially budget (the largest military budget in the world) but also by national cyber industrial capability (the largest and most powerful in the world) and the cyber-trained workforce (arguably the best trained in the world).

One important aspect of these leading organisations is that while they have shown considerable continuity in broad terms (with the JCS established in 1947), they have been adjusted at various points to provide a greater voice for existing, expanded or new capabilities, such as the Space Commander who was elevated to the JCS in December 2020. While cyber interests have never received the same prominence at the highest level, individual members of the JCS and parts of the vast organisations have represented cyber interests very strongly. This was particularly evident in the tenure of admiral Bill Owens, who served in a vice chief role from 1994–96. When it comes to the Unified Combatant Commands, the same aspects of continuity – while adjusting for new capabilities or interests – have been visible, but arguably are now more potent with the initial creation of Cyber Command in 2010 and its elevation to a Unified Combatant Command in 2018. It should be noted, however, that Cyber Command and its single-service component organisations (Army, Air Force, Coast Guard, Marine Corps, National Guard and Navy,) were not created out of thin air, but represented the consolidation and expansion of pre-existing organisational elements, some of which can trace their origins to at least 1998.

The profile of cyber-related 'causes' and interests within leading organisations will have a profound effect on the maturity levels that all aspects of cyber-related activities can reach. These leading organisations control budgets, development and capability choices, personnel

distribution, and training – not to mention warfighting and the requisite supporting joint structures. This consideration might be understood as the institutional weight of cyber issues, and within the US is arguably more mature than for any other country's armed forces, perhaps except for Israel.

Selected Lessons from China

The start date for China's military cyber development beyond the interests of the central military signals intelligence agency was around 2000. On the one hand, this was not too much later than the US start date around 1992. However, on the other hand, the foundations for cyber military power in each country in the 1990s could not have been more different – in ICT education and training, in the domestic ICT industries, and in the familiarity of each country's military personnel with use of computerised systems across the diversity of military functions and mission. In spite of tangible progress, huge differences persist in informatisation by the People's Liberation Army (PLA) over the past two decades. In 2021 the IISS assessed that the US lead in these key underpinnings of cyber power would probably remain at least ten years ahead of China and that China could only catch up if it made radical changes in policy.[43]

Thus, the country's cyber military development has had to advance on two fronts since 2000: (1) organisational reform (doctrine, training, new units and command elements, and policy), an issue confronted by all countries and a main focus of this study; and (2) building a cyber-industrial complex for servicing PLA weapons and capability needs that could compete with those of the US and its allies. This second element is less visible in this study, but is nonetheless fundamental to China's vision of its cyber military power. It is, after all, military officers who must write the procurement plans and technical specifications for cyber-enabled weapons platforms, cyber defence systems, and advanced communication platforms. To do so, they needed considerable training, formal education and military experience using computerised systems.

Leadership Receptivity

In December 2000, the motivations and challenges were reasonably well addressed in a series of speeches, kept secret for ten years, by the general secretary of the Chinese Communist Party (CCP), Jiang Zemin, to the Central Military Commission (CMC), the top decision-making body of military policy. He said that country's ability to fight a modern information war was weak, but that this had become the main form of modern war.[44] Within three years (a somewhat protracted period, but normal for such a momentous change), China had amended its military doctrine from one of 'winning local wars under high tech conditions' to one of 'winning local wars under conditions of informatisation'.[45] It took another three years for the CMC to approve new training regulations for the PLA under that new doctrine. In 2006, Jiang called in a public speech for an 'information deterrent' to complement China's nuclear deterrent. Public statements by the PLA, including in biannual White Papers on defence, began to reflect the increasing interest of the PLA in the necessary reforms as an imperative of the evolution of military art, technological opportunity and defensive need.

In the first decade, the leaders had other priorities apart from comprehensive development of cyber military capabilities. These were informatisation in the economy as a whole, informatisation of internal security (especially for censorship and surveillance), and international cyber espionage in which the PLA began to play a role. Space assets to underpin information operations became a new priority, as did the acquisition of one-off cyber weapons. It is testimony to the weak industrial and skills foundations in China at the turn of the century that it had to call on US and other foreign corporations to provide the equipment and know-how to build these systems.

From 2010–15, the country made significant sequential advances in cyber military modernisation at a faster pace than the previous decade. In 2010, the General Staff ordered the creation of an 'information warfare base' in the PLA to organise cyber defence (the term 'base' here means an organisational locus that can be geographically dispersed, not a single location). Traditionally, these responsibilities and capabilities had been split between the PLA Third Department (3/PLA) and the PLA Fourth Department (4/PLA).[46] In 2011, the US Department of Defense reported the existence of China's first doctrine for integrated kinetic and information operations to disable enemy forces. The same

year, the PLA began cyber war exercises (presumably tabletop style), beginning with a group of 30 top-line professionals, and important reforms in communications systems and command and control. In 2013, the US reported China's intent to dominate the information spectrum. That same year, the CCP endorsed a comprehensive nationwide economic-reform programme that had significant military informatisation reforms, including a heavy focus on innovation in defence-information systems and industries. It was also in 2013 that leaks by Edward Snowden revealed the deep inadequacies of China's cyber defences. In 2014, the General Secretary of the CCP, Xi Jinping, declared China's intention of becoming a cyber power, and approved several hundred thousand personnel cuts to the PLA to accommodate the transformations needed. In 2015, China issued its first public 'military strategy' by that name, declaring that 'outer space and cyberspace are the new commanding heights of international security competition'. It made a corresponding and quite radical reform by establishing a new entity called the Strategic Support Force (SSF).

The country's wealth and rapidly growing ICT sector carried the PLA efforts forward very quickly, but by 2016 the CCP acknowledged that all of China's core technologies were still too dependent on foreigners.[47] As China was racing to catch up, the rest of the world was not standing still, a trend particularly visible in artificial intelligence (AI) and its military applications. China had failed after more than a decade of trying to build an indigenous operating system that could replace Western-supplied systems and was far behind global standards in the most advanced semi-conductors, essential components in military equipment, especially for cyber and space operations. The PLA's education and training systems, including the establishment of reliable R&D partnerships with non-government entities, were arguably decades behind the US practice. Weapon design and development, including in cyberspace, are core military functions, even if in most countries military input is not considered during the actual R&D. For this reason, the leadership radically strengthened its approach to 'civil military fusion'. By 2021, the leadership issued a new plan for the invigoration of the domestic cyber-security industry, a fairly clear recognition that this sector, on which most military cyber operations of a country depend, was not a match for that in the US.

Character and Depth of Military Cyber Transformation

We therefore have a legitimate question about the character and depth of cyber transformation in the PLA and its ability to conduct advanced cyber defence and advanced cyber offence. Organisational name changes, cyber espionage against weakly defended systems, and writing doctrines for cyber operations are all quite straightforward and relatively easy. However, China has faced a basic contradiction between its ambitions for military cyber transformation involving advanced cyber defence and offence and the available inputs in terms of knowledge, skills and scientific research.

There is very little public-domain data on how China is responding to these capability deficits through organisational reform in the PLA, beyond the overarching structures of the SSF. We can track trends in PLA educational institutions supporting growth in military cyber units. One of these is the Information Engineering University in Nanjing, the only institution in the PLA with the formal designation of national training base for cyber security. It shows marked improvements and changes of direction to match China's military cyber ambitions, but the pace of change has been gradual, building off a relatively low base. We also know that the Chinese leadership is quite dissatisfied with the narrow base of the country's cyber security industry compared with the US, a view revealed in government guidance in 2021 on quite radical improvements to the Chinese sector.[48] Since the US record in meeting skills shortages, in spite of its advanced position, is quite mixed, it would defy logic to imagine that the PLA has been able to transcend the more severe impediments it faces in the national cyber-education system to produce large cohorts of highly trained cyber warriors who can operate at the same level as their peers in the US armed forces.[49,50] When it comes to the officer corps, one of the few available studies of the quality levels suggests that it will be 2035–50 before the more senior officers have the broad range of talents and experience that will match the

leadership requirements of the information age, especially the ability to lead multi-domain operations.[51]

That said, a country's armed forces do not need a large pool of cyber specialists to be able to inflict serious damage through cyber sabotage of enemy communications or weapons systems, but breadth and depth of capabilities are essential for cyber defence (cyber security). As one analyst noted, the structure of the SSF 'will have a major impact on how its forces can be effectively employed during a conflict'.[52]

It is also worth noting that for operations against the Islamic State (ISIS), the US adopted a task force model (specially compiled teams of individuals from different agencies) and judged it to be so effective that it was extended into more recent offensive operations against Russia and China. There is little public knowledge about the organisation of China's SSF in this regard, though we can presume, based on our knowledge of Chinese military organisational history, that such flexibility and institutional cross-over is not common.

We do know that the PLA probably followed the model of US Strategic Command, rather than Cyber Command, in setting up its SSF. At best, it is likely that the Network Systems Department of the SSF, the main one responsible for defensive and offensive cyber operations, is involved in a slow but steady transition toward a hybrid model that has been shaped and constrained by the pre-existing organisations that SSF absorbed. In contrast, US Cyber Command, with new missions and new structures, may have benefited from starting with a relatively unencumbered organisational structure.

This argument is vindicated to some degree by the conclusion of a IISS study which found that the PLA had so far conducted far fewer offensive cyber operations than the Russian or US armed forces. The study concluded that China's leaders were probably less convinced than their American and Russian peers of the political utility and military effectiveness of such actions, or that they were not yet prepared to take the risk given the early stage of development.[53]

Selected Lessons from Australia

The civil–military relationship in Australia has been the key determinant of the pace at which the country made the initial move toward higher levels of cyber maturity. The potential was always considerable, but from 1996 to 2011, the necessary elements (high commitment in the armed forces and receptivity in the upper echelons of government) did not exist. Between 2011 and 2014, the armed forces made important psychological and conceptual shifts, but the political environment was lagging. Alignment of these factors did not occur until Malcolm Turnbull, a wealthy businessman more in tune with the information age than any of his peers before (or since), was elevated to the prime ministership in 2015. He had experience investing in and co-leading a start-up email company in the 1990s, had served as the communications minister for two years, and was the first Australian prime minister to use the term 'information revolution' while in office.

There have been two main foundations of the Australian potential since 1996: a powerful cyber-intelligence capability in the Defence organisation, nested in the Five Eyes partnership since the 1950s; and the country's well-developed digital economy, including its basic science and technology position and its education system. Of these, the latter (in both the economy and education) has not been as well supported as it might have been. The former benefitted from huge injections of money and government attention in response to the terrorist threat after 9/11 and the country's expeditionary wars in Afghanistan and Iraq in the names of fighting terrorism.

Leadership Preferences

The transition of the Australian Defence Force (ADF) to a digital powerhouse could have begun at any point between 1996 and 2011, given that the country and its armed forces are closely tied to the US in policy, military development and military technology. The US had begun its journey in the early 1990s, with its first fully developed military doctrine on Information Operations published in 1998, manifesting the concept of information dominance, a concept the ADF has never enthusiastically endorsed. There are three main explanations for the lack of sustained attention to the potential of information warfare by the ADF through this period.

Firstly, the ADF was at war in Afghanistan (since 2001) and Iraq (since 2003), a situation which was largely responsible for inciting occasional but deadly

terrorist attacks on Australians at home and abroad, including the loss of 202 lives (mostly Australian) in a terrorist bombing in Bali in 2002. The armed forces and the intelligence agencies, especially the Australian Signals Directorate (ASD), had urgent new priorities, one of which was the recruitment of Australian citizens with Arabic, Farsi and Pushtun language skills, not to mention intelligence analysts with expertise in these cultures adequate for combat operations against insurgents (Australian intelligence had been focused heavily on Indonesia since the 1950s). These wars also led to a flood of refugees heading to Australia, many through Indonesia, relying on human traffickers to get them there by boat. Australia's small navy and maritime surveillance assets were heavily committed. The ADF arguably could not have afforded the time to consider a shift to warfare on the information age in the way that the US had. It should be noted that Australian agencies, including its police but also military personnel, played a significant role in intelligence collection that led to the early capture of the Bali bombers.

Secondly, the political environment in the country was not conducive to more rapid development of cyber military strategies. The conservative Liberal Party of Australia, in power since 1996, was simply not in tune with the military operational opportunities presented by cyberspace beyond espionage. The information revolution was not something the LP thought about much. After the Australian Labor Party (ALP) came to power in 2007, there was greater recognition of the importance of the digital economy, but the change was not massive and it certainly had little impact on the ADF. The party became embroiled in leadership struggles which diverted attention away from serious military reform and led to their electoral defeat in 2013. Both major parties saw the concept of the building of national-defence industry capability, especially shipbuilding, as a measure of the quality of its stewardship. Due to their backgrounds, key ministers in this period were simply not prepared for the digital revolution in military affairs.

A third reason is that few military leaders were pushing for change. Almost none of them had any relevant background or experience. In the mid-1990s, the vice chairman of the US Joint Chiefs of Staff, admiral Bill Owens, visited Australia and briefed the military leadership on his concepts of information dominance that had already taken root in the US armed forces, but politicians, academics and journalists did not seriously engage with his ideas. The military staff colleges and personnel managers in the armed services did not respond significantly to the lead of their country's senior ally in military reform.

Institutional Cultures

A key turning point for the ADF transition was a 2011 policy paper, 'Australia's Future Joint Operating Concept 2030'.[54] It asserted that technical and social networks would be the locus of efforts by states to secure their interests as well as several other statements heralding the shift to information-related operations alongside classic kinetic efforts. This policy guidance paper shifted the debate within the Defence organisation and by 2015, senior officers in the ADF had become impatient for their political masters to adjust national strategy and budget accordingly. This happened in the drafting through 2015 of the Defence White Paper, which was released in April 2016, having been deferred until that time for non-defence political reasons. The government, by then under an LP prime minister, issued its first substantial national cybersecurity strategy in March 2016, at which time the prime minister revealed that the country had offensive cyber capability.

The near synchronous release in 2016 of the Defence White Paper and the National Cyber Security Strategy was to a large degree coincidental, but the linkage between the two policy areas was profoundly important. Government ministers and ADF leaders of all backgrounds could grasp the significance of keeping Chinese and Russian intruders out of Australia's networks – whether in business, sensitive security departments of government, or the country's universities – even if they did not identify closely with the offensive potential and force-structure impacts of military cyber capability. The government created a new ministerial portfolio for cyber security, and several other institutional innovations for better cyber security. While total funding package was modest (US$172m in 2016 USD over four years), there was growing awareness that

Australia needed an answer to escalating cyber espionage. The ADF interest was further buttressed by the announcements in 2015 of reform to military cyber policy in China, including the creation of its SSF and its recognition that 'outer space and cyberspace are the new commanding heights of international security competition'.

In November 2016, Turnball revealed that Australia had used cyber operations against the Islamic State in Syria and Iraq and that these 'are making a real difference in the military conflict'.[55] During a visit to Washington DC in January that year, he had observed that while the armed forces of the coalition were doing well in kinetic operations against the Islamic State, the coalition was losing the battle in cyberspace.[56] While talking largely of influence operations and propaganda, he observed that the 'cybersphere demands reactions as rapid as the kinetic battlefield'. At the same time, the government reversed a long-standing policy of playing down cyber threats to the country in its public statements when the minister for cyber security made a speech at the National Press Club warning Australians to be prepared for a 'cyber storm'.[57]

Organising for Cyber Military Capability

By 1 July 2017, the ADF had moved to set up its Information Warfare Division (IWD), led by a two-star officer with engineering, military communications and special-forces experience, who had completed a PhD in cyber security, specialising in system analysis, not long before his appointment.[58] The officer would report to a newly created post, the Chief of Capabilities Group, who would eventually hold the same rank as the Chiefs of the Army, Navy and Air Force and who would also hold authority over several other joint units, notably the Defence War College and the Defence Academy for officer cadets.

The transition was aided by the author of the seminal 2011 policy paper, 'Australia's Future Joint Operating Concept 2030', who by that time was serving in the main cyber intelligence agency, the ASD, as a deputy director. The structures announced in mid-2017 would evolve in subsequent years, as the IWD began to work out the operating relationships with the ASD and single-service units with cyber capabilities. This was also the commencement dates for in-depth development of cyber military doctrine. Through this process, the IWD and the ASD had to come to an understanding that the ASD would lead on offensive cyber operations with the support of ADF personnel. The mission of the head of the IWD settled into the 'raise, train and sustain function' assigned to the single-service chiefs.

Personnel Availability and Training

The ADF was well prepared at the highest strategic level for the transition to cyber forces, but many areas of policy, including the development of personnel structures and training, needed to be addressed. In the 2016 Defence White Paper, a plan had been announced to staff a new Joint Cyber Unit (JCU) with 1,000 people within ten years. This commitment carried a requirement to train many more thousands of military personnel in the ten years to reach that target for the JCU and to staff ancillary functions elsewhere in the ADF. Between 2015 and 2017, the ADF undertook some pilot training programmes at UNSW Canberra (which is co-located with the Defence Academy). In 2020, with the need for improved general cyber-security training, the ADF launched another pilot programme, delivered by a group of small private-sector providers set up and staffed by Australians. At the same time, more specialised and more sensitive training was being undertaken in collaboration with ASD and the US, a continuation of long-standing training and development relations between ASD and its main Five Eyes partners. A project with Israel's Elbit Systems beginning in 2019 included the provision of cyber ranges by Elbit Systems for ADF training. By 2019, a clear plan had been formulated to expand the ADF School of Signals to include cyber training of various sorts.

Cyber as Stand-off Capability

By 2020, there was another series of boosts to ADF cyber capability: more leadership engagement, substantially more investment, and the acceptance in defence circles and the ADF that cyber issues had moved to the centre stage of international security. By this time the ADF had also accepted that China should become the main orienting factor for the development of Australian military capabilities and

operational concepts. The government repeated its 2016 double act by issuing a defence-policy paper, called 'Strategic Update 2020', and an updated cyber-security strategy.

The rhetoric revealed the significance of the shift. For the first time in its history, Australia believed that stand-off military capability was within reach: cyber assets in continental Australia could be used to blunt enemy military preparations at great distances from the landmass. Prime Minster Scott Morrison used the term 'stand-off capability' with gusto in one of his public statements and the Strategic Update used similar language: 'more potent capabilities to hold adversary forces and infrastructure at risk further from Australia, including longer-range strike weapons, cyber capabilities and area denial systems'. There was also growing recognition of the value of cyber assets in grey-zone operations, now accepted as an additional refence point for military preparedness. The government also announced new investments in Australian space-based capabilities in order to secure the intelligence and reconnaissance potential demanded by offensive cyber operations.

Steady Incremental Gains

The ADF reforms announced in 2016 and 2017 were premised on a ten-year development plan but without the benefit of an agreed doctrine. By 2020, a doctrine of some kind was in place but it has not been publicly released. The spending plans announced in 2020 served to quicken the pace of cyber reform but did not provide for a rapid transition to integrated and comprehensive cyber capabilities in the armed forces outside of the ASD. The ADF will continue the steady expansion of its forces, refine its operational concepts and try to bring online the appropriate cyber workforce to execute the ambitions. There does not appear to be as of yet a publicly articulated vision of the full scope of Australia's military cyber ambitions.

Strategic Maturity in Estonia

The case of Estonia offers several lessons in developing strategic maturity. Firstly, prioritising civilian capacity over military capacity due to resource constraints can hamper cyber capability maturity in the near term, but can serve to accelerate strategic maturity in the longer run. Long-term vision and continuity among senior leadership is particularly crucial in this regard. Secondly, low adaptive capacity and cultural hurdles can be mitigated through a monopoly over the cyber mission and by focusing on issues of strategic depth via reserves. Thirdly, allied relationships can effectively be leveraged to gain operational experience and compensate for unfavourable geopolitical conditions and a small resource base. These relationships work best when they are mutually beneficial. Finally, institutional and capability developments – such as establishing the Estonian Defence Forces (EDF) Cyber Command and couching capabilities within NATO – are important for solidifying progress in strategic maturity.

Striking a Civilian–Military Balance

The establishment in 2018 of the EDF Cyber Command might appear like a late development for a country with Estonia's history as a victim of a crippling cyber attack in 2007. Yet, extensive groundwork had been laid prior to its creation that has facilitated greater strategic maturity vis-à-vis the cyber domain. While Estonia continues to emphasise its decades-long post-Soviet focus on building out and modernising its conventional military capabilities, its response to the 2007 distributed denial of service (DDOS) attacks were grounded in a whole-of-country approach and not focused primarily on the armed forces.

In the wake of the 2007 incident, Estonia conscientiously prioritised building civilian governance capacity at the expense of developing military frameworks. The first *Cyber Security Strategy* was published by the Ministry of Defence (MoD) in 2008 but set out a series of measures to protect critical information infrastructure; to reorganise and expand the national institutional framework dealing with cyber security; to increase national competence in cyber security through training and research; to improve the legal framework for cyber security; and to embark upon an ambitious programme of international engagement on cyber security questions.[59] The strategy did not explicitly assign a role for the armed forces.

This initial emphasis on non-military aspects ultimately led Estonia to develop robust positions on the applicability of international law in cyberspace that

contextualise military cyber operations. While Estonia's official stance is not significantly different from like-minded countries, it set about a diplomatic campaign with a level of commitment and passion matched by few others. Although the prioritisation of civilian initiatives delayed the military's cyber-strategic development in the shorter term, robust civilian frameworks have helped to accelerate the EDF's strategic maturation in the longer term. Importantly, because the MoD handled the 2007 DDOS remediation efforts and subsequently spearheaded the government's cyber-security efforts, senior civilian leadership supported the development of military cyber capabilities. Moreover, the continuity in leadership played an important role. For example, Jaak Aaviksoo, who was minister of defence from 2007 to 2011, became minister of education in 2011 but temporarily carried out MoD duties when then-defence minister Mart Laar resigned in 2012 after suffering a stroke. The subsequent minister of defence, Urmas Reinsalu, continued the MoD leadership's endorsement for greater EDF cyber capabilities. Although the Support and Signal Battalion within the EDF had been tasked with this cyber mission in 2009, a military role in cyberspace was officially acknowledged at the policy level with the release of the 'National Cyber Security Strategy' in 2014.[60]

Initiating Change Amidst Resource Constraints

Early strategic conversations over the EDF's role in cyberspace and expanding the scope of the Support and Signal Battalion were hampered by both the military's low adaptive capacity and cultural hurdles. On the one hand, the EDF has had relatively low levels of financial and human capacity. With an emphasis on building conventional military capabilities and a yearly average of under 6,000 total active-duty personnel, the EDF has had few resources available for pursuing a larger role in the cyber domain. Moreover, with no redundant capabilities, cyber operations were confined to the small pool of expertise in the Support and Signal Battalion. Therefore, there was no resource base for the battalion to operate on a greater scale.

On the other hand, although commanders and service chiefs were more than willing to delegate cyber responsibilities to the Support and Signals Battalion, military leadership, such as then-chief of defence general Ants Laaneots, embodied a broader cultural constraint on cyber-strategic maturity. Military leadership has traditionally come from the army, by far the largest and most dominant branch within the EDF. This dynamic has perpetuated a 'green-heavy' culture across the military, meaning an army-centric culture that focuses on strategic issues like territorial defence and frames discussions around cyber capabilities as 'guns and tanks vs. computers.' While this inadvertently facilitated longer-term maturity by consolidating cyber expertise in the Staff and Signal Battalion, it also led to the short-term strategic isolation of cyber capabilities.

Accordingly, with these resource and cultural constraints and the civilian-first approach, most military initiatives were focused on developing depth via reserve forces. Cyber units within the Estonian Defence League, the reservist component of the EDF, were preliminarily operational in April 2009, and the Cyber Defence Unit (later renamed the Cyber Defence League) was officially established in January 2011. The tide began to turn, however, with the creation of the Cyber Policy Department within the Ministry of Defence in 2014 to oversee civilian ICT service provision in MoD and the cyber capabilities of the Foreign Intelligence Service and the EDF. Just as important was that the department served as the centre of gravity for discussions over enhancing EDF cyber capabilities. Mihkel Tikk, the first to head the department, was a particularly effective champion who spurred debate over reorganizing EDF cyber capabilities. Tikk's background – an officer in the Estonian Defence League with extensive private sector and governmental IT experience – provided him with the bureaucratic and political capital to cultivate momentum towards what would eventually become the EDF Cyber Command.

The Importance of NATO

Estonia has overcome obstacles to strategic maturity in large part by leveraging its membership in NATO at both the multilateral and bilateral levels. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), established in Tallinn in 2008, has played a particularly important role. Although the CCDCOE did initially divert strategic attention away from the national context and shrink the EDF's pool of resources

– personnel from the Support and Signals Battalion were needed to staff the new centre – Estonia has used the CCDCOE to couch its longer-term developments within NATO frameworks. The CCDCOE and its publication of the 'Tallinn Manual', though an unofficial collection of scholarly views, were major influences behind the 2014 'National Cyber Security Strategy', and the document explicitly stated that the EDF's cyber capabilities were to be developed for collective defence purposes under NATO.[61] Moreover, the CCDCOE has acted as an important staging ground for NATO's cyber exercises, such as the annual Locked Shields exercise.

This international aspect of Estonia's military cyber capabilities was an important dimension behind the initiative to establish the EDF Cyber Command in 2018. For example, in 2014, Estonian chief of defence general Riho Terras had offered NATO the use of the cyber range associated with the Support and Signal Battalion.[62] However, advocates of creating a new standalone Cyber Command rightly pointed out that the Support and Signal Battalion did not possess the scope or scale necessary for coordinating and integrating cyber capabilities with NATO and its other members.[63] With the official stand-up of the EDF Cyber Command in 2018, Estonia has continued to tie its strategic development to NATO, and in particular its use of offensive capabilities: it is one of five member states that has announced it will make available to NATO its sovereign offensive cyber effects.[64]

In conjunction with the domestic reorganisation of its military cyber capabilities, Estonia has increasingly turned to bilateral partnerships with NATO members for greater strategic development. Its recent activities with the US serve as a prime example. In 2019, the Estonian Ministry of Defence and the US DoD began working towards a joint platform for securely sharing cyber-threat intelligence.[65] Both countries have also cooperated in 'hunt forward' operations. For instance, from 23 September 2020 to 6 November 2020, teams from US Cyber Command and EDF Cyber Command undertook a defensive operation on EDF networks to hunt, identify, and mitigate adversary malware. Operations like these provide the US with a clearer picture of adversaries in forward-operational contexts, and Estonia receives crucial network assistance and the dissemination of best practices from a more bureaucratically mature partner.[66]

Institutional Maturity in the UK

With the establishment of its National Cyber Force in April 2020, the UK presents an important case of maturity for institutional arrangements intended to coordinate military cyber forces with their civilian counterparts. Much like the US, the UK's institutional maturity has been facilitated by long-standing military access to the national level civilian-intelligence infrastructure, expertise, and capabilities. However, unlike the dual-hat arrangement between US Cyber Command and the NSA, the UK has pursued a more integrated institutional approach that includes a range of other agencies, such as the Secret Intelligence Service, in more formal ways than the US arrangements.

A number of lessons on institutional maturity are evident from the UK. Firstly, ongoing military modernisation efforts offer an important glide path for reconsidering both how to organise military cyber capabilities and the relationship between military cyber capabilities outside of the operations of the main cyber/signals intelligence organisation, in this case Government Communications Headquarters (GCHQ). Of note, GCHQ is a civilian-led organisation, its members are civil servants, and it reports to the foreign secretary. Secondly, resource limitations – particularly in terms of technical capability and human talent – can produce organisational solutions out of necessity, without necessarily addressing divergent cultures. Thirdly, operational successes and other feedback can provide validation for arrangements intended to increase institutional maturity.

Early Moves to Consolidate Cyber Capabilities

Despite the budgetary constraints that flowed from the 2008 financial crisis, the UK had begun to publicly acknowledge its desire to develop greater military cyber maturity. Accordingly, the 2010 *Strategic Defence and Security Review* alluded to both the coordination of the military's cyber elements, including reservist components, and the coordination of cyber capabilities with conventional ones.[67] The classified *Defence Strategic Direction* in 2011 tasked the Ministry of Defence and its Defence Cyber Security Programme with defining and structuring the armed forces' cyber responsibilities.

The initial reorganisation of military cyber capabilities occurred with the momentum of broader modernisation efforts that established Joint Forces Command in 2011; the command would reach initial operating capability in April 2012 and full operating capability in April 2013.[68] The Defence Cyber Operations Group (DCOG) was established in November 2011 alongside these larger changes. The DCOG included the military's Joint Cyber Unit at Cheltenham, hosted by the civilian GCHQ and the Joint Cyber Unit at Corsham that operated alongside the Global Operations and Security Control Centre. Control over these military units was officially given to the Commander of Joint Forces Command in January of 2013, and the commander subsequently established the Joint Forces Cyber Group (JFCyG) in May 2013 to direct these units along with information assurance units and the Joint Cyber Reserve components.[69] The UK armed forces are responsible for protecting their own networks, and this mission rests with what is now UK Strategic Command, the successor to Joint Forces Command.

Foundations and Feedback for a More Integrated Civilian-Military Partnership

The UK defence secretary announced an intention to develop offensive cyber capabilities in September 2013.[70] However, the majority of the skills, infrastructure, and capabilities for offensive cyber operations have traditionally been concentrated within GCHQ, not the armed forces. Senior leadership acknowledged that adequately carrying out the cyber mission in a military context would require coordination with GCHQ. Early conversations among civilian and military leaders were quick to discount the model used by US Cyber Command and the NSA. Due to the UK's relatively smaller scale of government and military organisation compared with the US, a consensus emerged around the view that it made little sense to have parallel organisations with a common authority, as is the case in the US. Instead of accessing civilian-intelligence infrastructure and capabilities to jump-start a parallel military capability, the leaders decided to intertwine military and civilian elements.[71] It could be argued that this outcome was not resources driven, but rather the result of the much closer relationship that inherently exists between intelligence agencies and cyber operations. To this end, the National Offensive Cyber Programme (NOCP) was established, as an institutional arrangement rather than an organisation, in 2014 and was publicly acknowledged in strategic documents and statements in 2015.[72]

Operational feedback provided important validation for the military–GCHQ partnership, including from cyber operations against ISIS in 2016. These operations successfully manipulated and disrupted ISIS's efforts online, including their communications and the group's control over drones. Some operations even resulted in the destruction of equipment and networks.[73] More consequentially, defence secretary Michael Fallon indicated that, as part of the effort against ISIS, offensive cyber capabilities were being integrated into military planning alongside conventional capabilities.[74] Only in 2017 would the Ministry of Defence acknowledge that the military was conducting offensive cyber operations against ISIS.[75]

Successes against ISIS lent new energy to conversations about creating a more formalised and integrated partnership between GCHQ and the military. Discussions only intensified through 2018 as officials increasingly emphasised cyber capabilities as part of a broader effort to respond to and deter Russian aggression.[76] But questions remained about the size and who would head the new configuration – a military officer, a GCHQ official, or both in rotation. Nevertheless, by September 2018 the government had planned to fund an organisation to replace the NOCP arrangement, a natural step to gain greater effectiveness and efficiency for both military and civilian efforts in cyberspace.[77,78] In 2019 officials confirmed that the new entity would be called the National Cyber Force.[79] At the same time, and with little resistance, military cyber capabilities underwent further consolidation within Defence Intelligence and Defence Digital as part of another modernisation push that led Joint Forces Command to become Strategic Command in December 2019.[80]

An Ambitious Reorganisation

In November 2020, government officials confirmed the existence of the National Cyber Force and that it had been operational since April of the same year. This new partnership between GCHQ and the military is currently headed by a GCHQ official and contains other

elements from the Ministry of Defence and the Secret Intelligence Service (MI6). Although GCHQ provides the current commander, the Ministry of Defence will ultimately contribute a greater amount of funds and the workforce. The National Cyber Force intends to expand from its current size of 300 people to roughly 3,000 within ten years; however, this goal is likely to face severe budgetary constraints stemming from the COVID-19 pandemic.[81]

With the establishment of the National Cyber Force also came a broader mission scope for the armed forces. In addition to combatting hostile-state threats and terrorism, the National Cyber Force has the ability to disrupt a range of criminal activity. Balancing intelligence, military and law-enforcement goals will remain a challenge. While the new organisational arrangement does not eliminate possible conflicts over missions – or the potential for tension between GCHQ and the Ministry of Defence over authority for specific operations – it does allow for both the foreign and defence secretaries to work together to harmonise differences. More broadly, the expanded mission set is also coordinated by a ministerial group to ensure coherence with other government efforts in cyberspace and to help fulfil the UK's pledge to contribute sovereign cyber effects to NATO operations.[82]

Capabilities Maturity in Israel

The Israel Defence Forces (IDF) maintains robust cyber capabilities, including intelligence-based and offensive capabilities. The case of Israel provides several important takeaways regarding capability maturity. First and foremost, international partnerships can be an important conduit for increasing the scale and reach of existing cyber capabilities and expertise. Secondly, operational experience is a crucial avenue for developing increasingly complex capabilities that build off previous efforts. Thirdly, strategic developments can provide additional impetus for capabilities maturity by contextualising the role of cyber operations and directing new funding to cyber forces. Finally, establishing a cultural dominance over the cyber mission can have two opposing effects on capability maturity. Cultural dominance can have positive externalities by rewarding creativity and by aligning military and private sector-capability developers. At the same time, however, capability maturity can encounter cultural barriers.

Israel's military cyber capabilities are primarily held by Unit 8200 under the Military Intelligence Directorate and by the Joint Staff's Command, Control, Communications, Computers and Intelligence (C4I) Directorate. Although the C4I Directorate has moved to incorporate active cyber defence into its traditionally defensive mandate, Unit 8200 has been the primary locus for the IDF's cyber-capability development. Although these capabilities are not explicitly acknowledged, officials have alluded to their existence in the context of a full-spectrum approach to the cyber domain.[83,84] As with many countries, Israel's military cyber capabilities have grown out of signals intelligence, which have traditionally been the purview of Unit 8200. Both technological change and geopolitical disruptions, such as the Arab Spring, have pushed Unit 8200 to develop and use cyber capabilities.[85]

Amplifying Effects through Key Partnerships

While Israel has become highly capable in cyberspace, it lacks the global reach of other countries like the US and the UK. As such, a combination of partnerships – with countries like France, Singapore, the United Arab Emirates, the UK and the US – and operational experience and experimentation have been crucial for the continued maturation of its cyber capabilities.[86] Israel deployed cyber capabilities as early as 2007, when the IDF reportedly infiltrated and manipulated anti-aircraft radars in support of an air raid against Syria.[87] Unit 8200, in particular, has been linked to several high-profile cyber operations and the development of increasingly complex capabilities. Notably, this includes operations that produced and employed Duqu, Stuxnet and Flame malware, which were all publicly discovered between 2010 and 2012. Duqu was used to obtain the blueprints of Iran's nuclear programme, while Stuxnet was used to compromise and disrupt the industrial control systems of Iranian nuclear centrifuges (an earlier version was used to map vulnerabilities of the Natanz plant). Like Duqu, Flame was also used to collect intelligence on Iran's nuclear programme.[88]

There are several dynamics worth highlighting from these operational examples. Firstly, the development of each tool – Duqu, Stuxnet, and Flame – was a massive,

multi-year undertaking that occurred in cooperation with the US. For instance, the Stuxnet worm is reported to have been in development since 2005, and Duqu is suspected to have been developed at the same time by the same group of programmers. Secondly, they provide evidence of Israel's ability to move from network exploitation (Duqu) to network disruption that produced physical damage (Stuxnet). Thirdly, these operations, while different in scope, show increasingly complex programming skills that built on previous efforts. For example, Flame shared important features with Duqu and Stuxnet but contained at least 20 times more code than Stuxnet and was more difficult to detect than Duqu.[89]

Developing the Strategic Setting for Cyber Capabilities

Such operational experiences have occurred against the backdrop of modernisation initiatives, of which the development of greater cyber capabilities was an important part. While cyber capabilities were identified as one of 12 competency areas in Israel's most recent push for military modernisation, which started in 2017 and was revised in 2020, developing a broader strategic vision for these capabilities has been a major priority since at least 2010.[90,91] Then-prime minister Benjamin Netanyahu – a supporter of cyber as both a general-purpose innovation and a means of imposing costs on Iran, the primary strategic threat – asked Major-General (Retd) Isaac Ben-Israel, the Chairperson of the National Council for Research and Development in the Ministry of Science, to review and develop cybersecurity policy recommendations. This move eventually launched the National Cyber Initiative and resulted in the country's National Cybersecurity Strategy of 2011. Several governmental changes ensued, including the establishment of the Israel National Cyber Bureau (INCB) within the Prime Minister's Office to implement the strategy and coordinate inter-agency efforts. By 2017, the INCB had been combined with the recently created National Cyber Security Authority (NCSA) to form the Israel National Cyber Directorate (INCD).[92]

These changes to civilian agencies coincided with the 2015 release of the IDF's first publicly available defence strategy. The strategy recognised cyberspace as a military operating domain and portrayed military cyber capabilities, both defensive and offensive, as an important component of intelligence and defensive and deterrent efforts.[93] This helped accelerate Unit 8200's move from signals intelligence to cyber and cement it as the epicentre of IDF cyber capabilities with increased funding. Although the IDF had established the Cyber Defence Division – previously a cyber headquarters under the Deputy Chief of the General Staff – within the C4I Directorate in 2015, the centralisation of capabilities under Unit 8200 led to a downsizing of the C4I Directorate.[94] In addition to new financial limits, by 2017 the leadership of the C4I Directorate was culled from four brigadier generals to three.[95] Although centralising capabilities within Unit 8200 forefronts the inherent tension between cyber intelligence equities and producing effects that can impede strategic maturity, it has undoubtedly contributed to greater capability maturity.

Cultural and Technical Dominance within the Military Ecosystem

One effect of the consolidation and maturation of cyber capabilities within Unit 8200 has been civilian intelligence agencies relying on it. Because Unit 8200 collects roughly 90% of Israel's intelligence, both Shin Bet and Mossad cooperate with it extensively and there is military involvement in most major Mossad operations.[96] Unit 8200's capabilities are so substantial that, although the INCD manages national cyber-defence in peacetime, the IDF becomes the primary coordinator of national cyber efforts during crises.[97] These roles have also meant that Unit 8200 can also garner greater funding from the MoD Directorate of Defence Research and Development Directorate (Maf'at), which can allocate funding independent from requests made by IDF services and branches.

Perhaps the most unique factor influencing the IDF's cyber capability maturity is the organisational culture of Unit 8200, which emphasises creative experimentation and ferments relationships with the country's civilian technology sector. Unit 8200 faces few legal hurdles and weak civilian oversight in conducting offensive cyber operations; concomitantly, Unit 8200 prides itself on operational flexibility. As a result, the commanders of Unit 8200 generally delegate high levels of operational responsibility to troops and expect creativity from them.[98] On the

one hand, such an organisational culture rewards the production of effects. For instance, in 2020, members of Unit 8200 received medals for carrying out an operation against part of an Iranian port's infrastructure facilities, a retaliation for Iran's successful cyber operation on several of Israel's water-treatment facilities.[99] On the other hand, this culture has influenced personnel who have transitioned into the private sector after leaving active-duty military service. Reporting suggests that a number of former personnel have gone on to either launch technology start-up companies or take prominent positions in more established firms. With so many IDF alumni active in the private sector – and with mandatory reserve duty until age 50 – the technology section of Unit 8200 has developed close ties with the country's digital sector. These connections have facilitated both the maturation of military cyber capabilities and the further growth of the country's digital-security sector. Companies develop new technologies and capabilities which the military can test in live-fire exercises or in operational settings; some capabilities are then refined for further military use or are pushed back into corporate settings for release on the global market.[100]

Worth noting, however, is that the cultural and capability dominance of Unit 8200 with respect to cyber operations has prevented the development of greater institutional maturity for the IDF. Although there exist several independent cyber units across other IDF branches that can potentially spur competition and innovation, constraints on maturity are seen mostly clearly in Israel's failed attempt to create a unified cyber command that would encompass both defensive and offensive capabilities. In 2015, then-chief of the General Staff of the IDF, Gadi Eisenkot, initiated plans to combine Unit 8200 and the C4I Directorate into a single, unified command that would maintain responsibility for the full spectrum of cyber operations. Rigorous debate and negotiation ensued within the IDF and, by 2017, the proposal was abandoned. Eisenkot claimed that the initiative failed due to conceptual and technical disagreements over combining the defensively focused C4I Directorate with Unit 8200.[101] However, it is likely no coincidence that the idea was scrapped in the same month that Lt. Gen. Aviv Kochavi – a former chief of the Military Intelligence Directorate, which oversees Unit 8200 – was appointed Deputy Chief of the General Staff. Such cultural and bureaucratic resistance to a merger from Unit 8200 is likely winning out with allies in leadership positions, particularly given that Kochavi replaced Eisenkot as Chief of the General Staff and was still occupying the position in October 2021.[102]

Conclusions

No country's armed forces have reached full cyber maturity. Unsurprisingly, the United States has made the most progress across the three aspects – strategic maturity, institutional maturity, and capability maturity. The reality for most countries, however, is that maturity unfolds unevenly across these categories over time. As our case studies have also shown, maturity is dynamic, and advances in one dimension of maturity can often create tensions with initiatives in other dimensions. When progress towards greater cyber military maturity does occur, it is often due to the efforts of entrepreneurial individuals who act as champions for cyber-related reforms.

We have identified four main governance factors and three organisational influences that enable or constrain the development of cyber military maturity. In our judgement, these seven factors represent the major shaping forces that governments and analysts must consider when assessing the cyber maturity of armed forces. For governance factors, civilian-military relations of cyber operations, senior political-leadership receptivity to cyber issues, broader 'military modernisation' efforts, and alliances and international partnerships are all critical dynamics that shape both the processes and potential outcomes of maturity initiatives. Competing cultures (within the military and between the military and intelligence agencies), the military's adaptive capacity, and operational experiences in the cyber domain represent three crucial organisational factors that influence how, when, and to what extent a military can mature.

Policy leaders need to be mindful of the speed of their policy measures, the extent to which these can accelerate improvements in capability (continuous expansion), and the ways in which they can maintain momentum for cyber military reform in the face of competing pressures. Above all else, policy leaders must have credible mobilisation plans for military cyber operations, either for wartime or in support of the civil authorities for lesser contingencies. For most countries these mobilisation plans will need to be alliance-based, since independent or sovereign cyber military capability will remain a distant horizon for at least a decade, probably longer.

We remain at the dawn of the cyber age. In large part, strategic, institutional, and capability developments for armed forces are just beginning. The framework for assessing cyber-military maturity advanced in this paper can be a useful tool in understanding the current and future trajectories of conflict and competition in the cyber domain.

Appendix: Explaining the Military Cyber Maturity Impact Matrix

Few works engage in explicit analysis of cyber military maturity; most focus on strategic dynamics or operational histories. An early attempt to grapple with maturity surveyed military cyber capabilities in the European Union by utilising a seven-dimensional model.[103] Developments along each dimension were assessed as either non-existent, in initial stages, defined, balanced, or optimised. Despite a holistic approach, the study suffered from substantial bias, as analytical judgements relied on interviews and questionnaires with officials responsible for developing cyber maturity. Recent academic works have made progress in conceptualising certain aspects of maturity. Smeets portrays the development of military capacities for offensive cyber operations as a business lifecycle of seed and development, start-up and launch, growth, expansion, and full maturity.[104] Similarly, Blessing explains how the institutional dimensions of military cyber forces evolve and mature over time.[105] Ormrod and Turnbull advance a more comprehensive framework that incorporates technical capability, strategic planning, and organisational behaviour and emphasises levels of trust on the battlefield. Maturity spans five potential stages: basic awareness, information assurance, information superiority, behavioural defence, and mission assurance.[106] However, this model cannot capture the reality that some militaries may make considerable progress in some aspects of maturity but not others. We therefore propose a conceptualisation of cyber military maturity that allows for variation in progress across different dimensions.

Strategic Maturity

The degree to which military organisations and their leaders have outlined concrete plans to develop cyber capabilities in support of national level-security goals and have demonstrated the political leadership to implement declared goals.

Governance Factors

Senior Leadership Receptivity. The ability of senior civilian leadership (at the political level) to be enablers of strategic maturation hinges on two interrelated dynamics: their interest in considering the role of military cyber option and changes in composition of the leadership (who is in, who is out, who is rising and who is not).

While leadership interest is not necessarily a prerequisite, their openness to incorporating cyber capabilities alongside other, more traditional strategic levers of state power can be an important enabling condition for maturity (both in policy and budgetary terms). By 2021, the demonstration effect for most leaders of the expansion of cyber military operations and force elements globally will have been marked. An increased leadership desire to understand the role of cyber capabilities would likely shift the balance between cyber advocates and traditionalists. Specifically, it can help reorient dynamics of military advice, which might otherwise default to emphasise the utility of conventional means.[107] As curiosity surrounding cyber operations grows in senior officials, it can have ripple effects that push or encourage more in-depth strategic thought in military leadership about the role of cyber forces and capabilities.

The political dynamics inside senior leadership groups will shape the level of strategic maturity for military cyber forces. Changes via elections or appointments can act as a catalyst for strategic and doctrinal developments by bringing digital champions or other cyber-minded individuals into leading government positions. At the same time, turnovers in leadership can disrupt processes of strategic maturation if officials interested in cyber issues leave government circles.

It is the character of politics that leaders will be forced to decide how much political capital to spend to advance cyber-related reforms in strategy and force structure, or even to undertake cyber operations. Trade-offs, often resulting in suboptimal outcomes, will be a normal part of the process. This factor may account for a key finding of the International Institute for Strategic

Studies that strategic shocks have been a major driver of cyber reforms in national security policy.[108] The process need not be entirely rational since many leaders would not make a strong distinction between escalating cyber espionage and escalating capability of potential adversaries to conduct offensive cyber military operations in wartime. Governments have often pushed for the expansion of cyber capabilities or institutional reforms in response to exogenous shocks, but have generally lacked the knowledge or commitment to follow through on initial measures.

Civilian–Military Relationships on Cyber Operations. The structure of civilian-military relations, both at high levels and at the working level, plays a crucial role in the development of strategic options for cyberspace operations. The relative balance of power and authority between the political and military classes will shape those choices.[109]

Below the level of government-wide institutional and legal dynamics, the relationship between military cyber forces and civilian intelligence agencies that undertake cyber operations looms large for strategic development. Unlike military cyber forces, civilian intelligence agencies largely focus on and tend to prioritise information collection. Naturally, military cyber forces can and do collect intelligence. However, for military cyber forces, intelligence collection is generally subordinated to and supports gaining strategic advantages. Tensions can thus arise between civilian intelligence agencies seeking to elevate the strategic importance of exploitation and military cyber forces emphasising the strategic payoffs of disruption. In practice, because intelligence sources in cyberspace can (and often do) have multiple stakeholders across civilian intelligence communities, military-conducted cyber operations have the potential to sacrifice long-term intelligence gains at the expense of short-term tactical gains. Reconciling these trade-offs by developing frameworks for balancing intelligence gains and losses is an important enabler for greater strategic coherence and maturation for military cyber forces.

For militaries in advanced and/or consolidated democracies, legal oversight requirements and constitutional restrictions on certain offensive cyber operations underpin efforts to develop military strategies for cyberspace. Intimately related is a government's legal interpretation of sovereignty in cyberspace and the types of actions in the cyber domain that violate sovereignty. For instance, strategic development for a state that believes cyber operations do not violate sovereignty will look very different from the strategic trajectory of states that believe sovereignty is violated by cyber operations that produce effects, which will be different from a state with the position that any type of cyber operation violates sovereignty. Such legal interpretations carry direct implications for conceptualising out-of-network operations. In the first case, all types of out-of-network operations are strategically 'fair game'; in the second case, strategic development for out-of-network operations will probably primarily focus on exploitation. Strategic maturation vis-à-vis the role of out-of-network operations in the third case is likely to lag the other two.

Military Modernisation. Broader military modernisation efforts can provide important impetus and inertia for the maturation of cyber strategy. However, the effects of military-wide changes on strategic maturation are contextual based on the timeline of modernisation. The early stages of military modernisation reforms can stall or hamper the strategic maturation of cyber forces. Because military organisations, their relationships, hierarchies and capabilities are in flux, cyber doctrine is likely to be more transient in nature. Military cyber forces may thus rely on low-sophistication techniques and concepts at the early stages of modernisation.[110]

In contrast, strategic maturation can accelerate in the later stages of military modernisation. The solidification of institutional arrangements is generally accompanied by new military-wide and service-specific strategies and doctrines. As such, civilian and military officials are more predisposed to consider the cyber domain both as a part of joint-service and multi-domain operations and as an independent operational domain. In this context, institutional reforms that give cyber commanders a seat at the table can significantly advance strategic debates and contribute to cyber force maturation.

Alliances. Alliances and military partnerships between and among states can exert both direct and indirect effects on a cyber force's efforts to achieve greater strategic maturity. The opportunity for consultations, intelligence sharing, and joint exercises and operations among allied nations offer nascent cyber forces the ability

to directly learn from and borrow strategic concepts and frameworks from others. In this sense, alliances can perform a traditional informational role, in that they can provide information on common threats, the operating environment, and effective measures to counter threats. At the same time, however, varying levels of strategic and policy development among members can result in different understandings about the role of military cyber operations that can limit the transmission of information.[111]

Alliances can also act as an indirect catalyst for strategic maturation. Political friction among allies over out-of-network operations on allied networks has the potential to spur greater debate over potential payoffs and blowback of some offensive cyber operations.[112] Alliance membership adds this layer to the strategic calculus for cyber forces: producing effects on an ally's network to disrupt a third party, while operationally similar, will carry qualitatively different strategic and political implications than producing effects on a non-allied network. It is these implications that can drive the development of new or refinement of existing strategic frameworks for cyber operations.

Organisational Factors

Operational Experiences. Operational experiences provide the opportunity to put strategy into action. Testing novel concepts of operations 'in the field' is crucial for developing measurements of effectiveness and refining how military cyber forces execute their mission. Without operational feedback on new ideas and concepts, strategic maturation can stall.[113] Both live operations and exercises can relay important strategic information about the strategic utility of cyber operations as an independent tool, a force multiplier and an enabler for traditional kinetic operations.[114] Operational experiences across these contexts can contribute to greater strategic maturity, as commanders and other leadership can develop and test new concepts of operation. The lessons learned from operational experiences, however, are mitigated and complicated by the opaque signalling dynamics of cyberspace and pre-existing bureaucratic and cognitive biases.[115]

Military Adaptive Capacity. A military's adaptive capacity – its ability to identify, explore and exploit disruptive strategic ideas by integrating them into its organisational functions while still implementing existing strategy – is a critical enabling factor for greater strategic maturity.[116] Larger militaries are likely to possess greater adaptive capacity than smaller militaries. However, the effect of adaptive capacity can be uneven across time.

Higher levels of adaptive capacity can promote strategic maturity in three ways. Firstly, militaries with high levels of adaptive capacity will generally possess more complex knowledge-transfer systems that can produce greater diversity of thought than in smaller militaries. Secondly, adaptive militaries tend toward redundancy. For example, in smaller militaries, cyber capabilities and planning are generally confined to a single command; in contrast, multiple combat services are likely to possess cyber capabilities in larger militaries. The redundancy of cyber responsibilities can facilitate the regular emergence of new and diverse strategic frameworks for cyber operations. Thirdly, the loose organisational coupling that accompanies adaptive capacity can increase strategic maturity by allowing for experimentation and innovation – and the failures that will inevitably accompany some of them – without impacting overall military performance and by providing entrepreneurial individuals with connections to experts across other military components.

At the same time, greater adaptive capacity does not ensure strategic maturation. The generation of new strategic frameworks requires adoption and implementation across the military. In this sense, the redundancy of cyber responsibilities is a double-edged sword, as it produces a greater number of veto players that can stifle strategic debates. Combat services can cling to their own specific strategies and doctrines at the expense of an overarching strategy, thus stalling implementation efforts after the idea-generation stage.[117]

Divergent Cultures. Conflicting cultures are particularly impactful for strategic maturation. Two fault lines are particularly salient. Firstly, military subcultures (such as service-specific cultures) can restrict the scope of strategic thought surrounding cyber operations. This is particularly likely in the early stages of strategic maturation, where high levels of uncertainty give combat services space to develop independent initiatives and frameworks for cyber operations that mesh with existing service missions and cultures.[118] One the

one hand, competing cultures and interest-claims vis-à-vis the cyber domain can hamper strategic maturity. A key impediment to strategic maturity in this sense is that cyber capabilities are mistakenly seen as an inexpensive substitute for conventional capabilities. On the other hand, reconciling disparate cultural approaches can contribute to greater maturity down the line, as each service can contribute unique insights on the cross-domain implications of cyber operations. A primary risk to service-driven strategic development, however, is that no cyber-specific culture emerges.

Where cyber-specific cultures have been developed, a different type of cultural rift can result from the organisational origins of cyber forces. Strategically, cyber forces that emerge from combat services are likely to favour overt action and operations that have a more immediate impact on the battlefield than those favoured by intelligence agencies, which may prefer continued intelligence collection and exploitation over disruption. This latter preference was very much in play in US choices concerning operations against ISIS up until 2016. Those cyber forces originating in military-intelligence circles are likely to emphasise exploitation, information collection and covert operations.[119] Reconciling these competing lenses for cyber operations is crucial for developing frameworks to mitigate the trade-offs of exploitation and disruption. Those cyber forces that are unable to do so will find limited room for further strategic maturation.

> The degree of effectiveness with which a military organisation has harmonised its planning, force preparedness and execution to deliver cyber operations in support of national level security goals in key theatres of operations.

Governance Factors

Senior Leadership Receptivity. In the early stages of establishing a cyber force, support from senior leadership is crucial for maintaining implementation momentum. This support can range from active advocacy to non-interference as a new command is created. Interference or obstruction from senior leadership is a death knell to establishing a cyber force or implementing organisational reforms. As with strategic development, consistency and turnovers in senior leadership have important impacts on institutional maturity. When senior leadership opposes creating or expanding the scope of a military cyber force, turnovers via elections or appointments can serve to bring in new advocates.

However, turnovers can stall the development of institutional maturity even when both outgoing and incoming leaders support cyber-force initiatives. In these instances, changes in administrations and/or staffing inevitably delay organisational implementation efforts by months or years. From a purely developmental perspective, greater institutional maturity for a cyber force is gained through sustained support from senior leadership that goes through few changes or turnovers. One important way that this support can manifest is in initiatives to increase both the number of cyber warriors as well as their overall training levels.

Civilian–Military Relationships on Cyber Operations. Disentangling and defining the relationship between military cyber forces and civilian intelligence agencies are key elements in moving from lower to higher levels of institutional maturity. Rivalry and/or conflict between civilian and military elements can hamper the military's ability to develop an independent organisational footprint and conduct its own operations in cyberspace unimpeded. Reconciling the civilian–military relationship to facilitate maturity can take several forms. For instance, the institutionalisation of information sharing – such as the colocation of military and civilian intelligence Computer Emergency Response Teams (CERTs) for crisis management and incident response – can remove a hurdle to achieving greater military maturity.[120] Formalising cooperation can also occur at higher levels, such as through regularised inter-agency groups or panels. These settings provide a basis for deconflicting military targeting cycles with civilian intelligence collection and discussing the strategic trade-offs of using certain cyber weapons, such as how using a specific tool to produce military effects could devalue other tools in an intelligence setting.[121]

In addition to removing barriers, defining organisational relationships between civilian intelligence agencies and military cyber forces can serve to accelerate

institutional maturity. Many nascent cyber forces lack the infrastructure and expertise of their civilian counterparts, which are more likely to have the robust signals intelligence capabilities that are crucial to cyber operations. The colocation or integration of civilian and military elements – in a single building or even under a single command – can provide military cyber forces with access to more developed infrastructure and expertise. Although such arrangements have the potential to create a dependence on civilian infrastructure, access to well-developed civilian agencies can help offset the costs of early maturation efforts.

Military Modernisation. The reorganisation or consolidation of cyber capabilities as part of military modernisation efforts offers a potential pathway for greater institutional maturity. Modernisation can draw cyber personnel and capabilities from across the military into a single command structure that can produce a more coherent approach to executing the cyber mission. Such reorganisations can also be accompanied by the standardisation of operating procedures that help eliminate duplicated or even contradictory initiatives in the cyber domain. The consolidation of cyber capabilities into one command has the added benefit of creating a centre of gravity for budgetary considerations.

Moreover, military-wide modernisation efforts have the potential to redefine hierarchical relationships of cyber commanders vis-à-vis conventional force commanders. In particular, pushes for modernisation have the potential to create new mechanisms for integrating cyber-force components into conventional operations. This can be a critical step for pre-existing cyber forces with moderately high levels of maturity for their independent operations, but have not yet gained experience co-deploying cyber capabilities with traditional kinetic ones.

Alliances. Alliances can be a crucial source of information for achieving greater institutional maturity, particularly when cyber forces are in the early stages of organisational operation. Consultations between and amongst allies can provide critical insights for states that are in the early stages of standing up new military cyber commands. In particular, consultations provide exposure to the trade-offs of different organising principles for cyber forces, such as trade-offs related to creating an independent branch, an independent service, or a joint-service cyber force. Allies can use this information to accelerate institutional maturity by planning for and avoiding many of the early 'growing pains' associated with building new organisations. Attempting to meet allied inter-operability standards can also provide a political basis for expanding the bureaucratic resources for cyber forces to close the gap with more advanced allied cyber forces.

Organisational Factors

Operational Experiences. Like with strategic maturation, operational experiences can provide important feedback to military cyber forces about how to conduct its mission. Just as important, however, is the fact that operational experiences can provide 'proof of concept' to cyber commanders, commanders of conventional forces, and to senior governmental leadership that justifies the existence or growth of cyber forces. Joint operational ventures can help link the effects of cyber operations to the strategic priorities and outcomes of military commanders of conventional forces. Operational successes can thus serve to reduce military commanders' uncertainty over the implications and payoffs of cyber operations. Reduced uncertainty can in turn drive commanders to incorporate cyber effects into future operations. This provides a basis for the maturation of cyber forces through bureaucratic expansion and the institutionalisation of relationships to other military commands.[122]

Military Adaptive Capacity. The military's adaptive capacity shapes the way cyber forces and their implementers approach building institutional maturity. The key tension here is between devoting resources and attention towards operational effectives and building and integrating a cyber force into the broader military bureaucracy.

In militaries with low levels of adaptive capacity, the pathway to maturity will likely entail mapping cyber forces onto existing organisations and prioritising bureaucratic integration before building out the cyber force's mission and operational effectiveness. Organisational constructs for cyber forces will thus look to access existing knowledge and expertise to build the cyber mission. Once established, however, the lack of redundant capabilities can actually serve

to accelerate institutional maturity: once the strain on resources has been justified, cyber forces face little competition over the cyber mission itself. This suggests that militaries with little adaptive capacity face a high bar for institutional innovation, but a potentially easier path for implementation.

Conversely, militaries with higher degrees of adaptive capacity are likely to build greater maturity by emphasising the operational effectiveness of a cyber force before considering bureaucratic integration. The looser organisational coupling and more complex knowledge systems of a highly adaptive military enable greater risk-taking for institutional innovations. However, the redundancy of cyber capabilities across a military can hinder subsequent attempts at implementation, as prevailing bureaucratic interests may seek to prevent the rise of a competing organisation. As such, militaries with high adaptive capacity are likely to face the backlash of organisational politics in later stages of implementation.[123]

Divergent Cultures. Cultural clashes over the cyber mission within the military present a major obstacle for cyber forces to develop greater institutional maturity. For one, intra-military rivalries that stall organisational reforms can emerge. When multiple services see cyber operations as part of their existing missions, conflicts over 'the right way' to define and carry out the cyber mission can prevent the organisational consolidation or merger of cyber elements across the military. Even when reorganisations are not the goal, competing cultural frames can limit bureaucratic efforts to integrate existing cyber capabilities more effectively with each other and with conventional capabilities.

In addition to cross-military cultural dynamics, the culture within an organisation impacts prospects for greater institutional maturity. When culture defines and emphasises cyber operations in the context of geographically-based domains, organisations risk isolating and reducing the cyber mission to support functions. This will be reflected in command structures and the separation of analogue and digital ways and means that place limits on institutional maturity.[124]

At a broader level, the generally hierarchical nature of all military cultures can hamper the integration of cyber tools into lower levels of command. More institutionally mature forces will have the bureaucratic capacity to incorporate cyber 'all the way down' their organisational charts. In particular, the delegation of operational decisions further down chains of command can build on existing expertise and patterns related to intelligence, electronic warfare, and space-based efforts. A key hurdle to the devolution of command is a natural tendency to over-classify cyber capabilities, thereby concentrating knowledge and control at higher levels of command. As a result, predispositions to rigid hierarchy and over-classification can prevent organisations from develop greater maturity.

> The extent to which cyber forces have developed defensive and offensive cyber options and the levels of human skill required for utilising them in key theatres of operations in a manner corresponding to strategic intent and the organisational demands.

Governance Factors

Senior Leadership Receptivity. While senior leadership is unlikely to possess detailed knowledge of cyber tools and operator needs, top leaders are positioned to direct funding towards recruiting new personnel and researching, developing and acquiring new capabilities. To be sure, robust research and development processes contribute directly to the maturity of cyber capabilities.[125] None of these efforts are short-term paths to maturity. Therefore, senior leadership facilitates capability maturity when leaders take a longer-term view of amassing cyber personnel and weapons – a longer-term view that should look past their own tenure. A crucial component of this facilitation role is confidence in the broader civilian cyber-defence industrial base. As with the other dimensions of maturity, consistency or turnover in leadership posts can either open new windows for or disrupt cyber force implementation efforts.

Civilian–Military Relationships on Cyber Operations. The outright prioritisation of civilian intelligence capabilities over those of military cyber forces is an obvious barrier to maturity. However, a more nuanced view of maturity emerges when considering the interdependence of civilian and military capabilities.

Mature military cyber-capabilities often require significant intelligence work prior to deployment. In this sense, the primary tension affecting maturity is between military targeting requirements and the devaluation of civilian intelligence agencies' capability portfolio. Militaries working towards greater capability maturity must be able to establish network access across a variety of potential targets prior to an attack. Many of these access efforts will rely on civilian intelligence agencies which possess their own relatively mature cyber capabilities. Moreover, the costs of cyber capabilities increase substantially when determining potential collateral damage for an attack to comply with the laws of armed conflict.

Many military targets, however, will never actually be attacked. Therefore, the payoff of attacking one target must be large enough to offset the costs of potentially wasting capabilities on the preparation of other targets that are not attacked.[126] Civilian intelligence agencies that do not view this as a worthwhile trade-off will be reluctant to contribute capabilities. In other words, the opportunity costs for military targeting become too high: civilian intelligence organisations, which serve a variety of national-security objectives, will not want to waste capabilities that could be used for their own intelligence ends. Intelligence agencies may thus take steps to guard capabilities – such as through over-classification – that negatively impact military-capability maturity. Achieving greater capability for military cyber forces therefore requires frameworks for mitigating and equitably distributing the sunk costs of deploying multiple tools to gain widespread access.

Military Modernisation. The early stages of modernisation efforts are likely to see little change in the capability maturity of cyber forces. While military modernisation reforms can bring military cyber capabilities under the purview of a single command, there can be significant delays in developing the organisational knowledge needed to effectively combine and utilise previously disparate capabilities. In the longer run, however, modernisation can facilitate capability maturity in two main ways. Firstly, reforms can place an emphasis on modernising information and communications technology across the military. As such, new acquisition opportunities can emerge that accelerate the technological capabilities of cyber forces. Secondly, and related to institutional maturity, modernisation has the potential to enhance human capabilities by opening new billets for cyber-specific positions and creating new career tracks. Modernisation is thus one mechanism through which cyber forces are better able to recruit new and retain experienced personnel.

Alliances. Multilateral and bilateral relationships with allied nations can be an important source for the maturation of cyber capabilities. Capability development – and more specifically, the development of human capabilities – can disproportionally benefit from participating in multilateral or bilateral exercises. This is particularly true for militaries that lack significant domestic-staging abilities for exercises. Such ties and relationships, however, are unlikely to advance the maturation of technological capabilities. The primary reason is due to the distinct nature of the political economy of military cyber defence. Unlike in traditional domains, where allied states are more likely to transfer arms and weapons systems but not the knowledge of how to use them, the cyber domain predisposes states to transfer knowledge to allies but not their 'weapons'. Doing so would expose strategically important exploits as well as the sources and methods used to gain such exploits.

Organisational Factors

Operational Experiences. Cyber forces can develop greater capability maturity from operational experiences – including exercise and live field operations – in two main ways. First and foremost, exposure to different techniques and tools have cost-reduction and learning-curve effects. Many capabilities possess common vulnerabilities, exploits, and proliferation techniques. For instance, Stuxnet has been linked to both a predecessor worm named 'Fanny' and to subsequent tools like Duqu and Flame.[127] Thus, experience with one capability can inform future defence efforts.

Likewise, experience can aid future offensive operations. Malware and other capability developers within a cyber force can learn from the work of adversaries and even redeploy an adversary's tool after modifying it.[128] In these ways, operational experiences can contribute to overall capability maturity by lowering the costs associated with developing, deploying, and defending against a variety of cyber weapons.

Secondly, operational experiences provide important feedback on the impacts of capabilities. On the one hand, this feedback can be contextual: the effectiveness of a capability can differ based on the types of defences and network architectures it faces. Such information lends itself to greater capability maturity through the development of tailored cyber tools. On the other hand, operational experiences shed light on the second- and third-order consequences of a capability, many of which may be unintended effects. The ability to account for multiple-order effects past the immediate impact of cyber tools evidences greater capability maturity.

Military Adaptive Capacity. While cyber capabilities are generally high-demand, low-density capabilities across militaries, adaptive capacity helps to shape and develop capability maturity efforts. While overall resource levels are certainly important – the militaries of great powers will have the resources to develop highly impactful cyber capabilities – the ability to adapt existing resources and experiment with new ones is just as important.

Higher levels of adaptive capacity are likely to facilitate the early stages of capability maturity for a military and its cyber forces. The costs of developing capabilities are concentrated in tool development, with relatively fewer costs after initial development.[129] As such, militaries with greater adaptive capacity are better able to bear the early costs of capability maturity. Complex knowledge structures and redundant bureaucratic focus on the cyber mission will help facilitate the emergence of new and robust capabilities. Looser coupling can also incentivise experimentation with new technologies and deployment procedures. Conversely, with fewer sources of capability development, militaries with low adaptive capacity are likely to struggle to develop baseline levels of capability maturity.

In the longer term, however, greater adaptive capacity can present hurdles to greater capability maturity. On the one hand, redundancy can foster a lack of interoperability: capabilities and systems emerging from different combat services can create an incoherence that intensifies resource requirements and prevents greater maturity.[130] On the other hand, the loose organisational coupling that is generally associated with adaptive capacity can lead to incrementalism. Loosely coupled militaries can struggle to effectively or efficiently implement widespread updates or upgrades to information and communication technologies that can be critical for later stages of capabilities maturity. In contrast, the tighter coupling of militaries with low adaptive capacity can facilitate the later stages of capability maturity. The acquisition, experimentation, and macro-development of capabilities in such militaries will be more centralised with fewer bureaucratic barriers.

Divergent Cultures. Cultural dynamics can influence perceptions of opportunity costs for developing cyber capabilities when resources could be used for other missions. This can play out in several ways, two of which are worth emphasising. Firstly, greater capability maturity can be inhibited when military commands do not define the cyber mission as a component of their own respective missions. As a result, the opportunity cost of contributing to capability development is too high and is seen as the responsibility of a specialised organisation (like a standalone cyber force) that lacks adequate resourcing. Secondly, multiple organisations and combat services can develop cyber capabilities, but only in support of specific missions. In this context, the capabilities pursued are the best 'cultural fit' for existing missions, and investments are curtailed for capabilities that exceed mission requirements. This can risk siloed capabilities and cross-service duplication that slows capability maturity.[131] Broader military culture also hinders capability maturity in terms of human capital. More specifically, the general notion of 'what a warrior looks like' is at odds with much of the potential pool of talent. Conventional cultural standards are therefore likely to make capability maturity harder to achieve.[132]

Notes

1 IISS, 'Cyber Capabilities and National Power: A Net Assessment', June 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

2 *Ibid*.

3 The seven aspects are strategy and doctrine; governance, command and control; core cyber intelligence capabilities; cyber empowerment and dependence (the digital economy and its ecosystem); cyber security and resilience; global leadership in cyberspace affairs; and offensive cyber capability.

4 This type of matrix comes in many variants. In our matrix, we have deliberately avoided the inclusion of developmental milestones that might equate to a level of maturity. Though that could be done as an evolution of this approach, it is hard to see how some elements, especially civil–military relations, might be reduced to some idealised pathway, let alone quantified. As noted in the text, the pathways are always country specific. They can only be understood as a specific combination of the elements in the matrix.

5 J. W. Kingdon, *Agendas, alternatives, and public policies* (Boston, MA: Little, Brown, 1984), pp. 188–93.

6 J. Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca, NY: Cornell University Press, 1985); B. Posen, *The Sources of Military Doctrine* (Ithaca, NY: Cornell University Press, 1984).

7 N. Dixon and G. Wawro, *On the Psychology of Military Incompetence* (London: Pimlico, 1976).

8 This point, 'in all phases of operations', was prominent in the US Cyber Commander's Vision Statement, 'Beyond the Build: Delivering Outcomes through Cyberspace', US Cyber Command, 2015, https://www.hsdl.org/?view&did=787006.

9 M. Evangelista, *Innovation and the Arms Race* (Ithaca, NY: Cornell University Press, 2019), p. 51; E. O. Goldman, 'Introduction: Military Diffusion and Transformation', in E. O. Goldman and Thomas G. Mahnken (eds.), *The Information Revolution in Military Affairs in Asia* (New York: Palgrave Macmillan, 2004) pp. 1–21; A. F. Krepinevich, 'Cavalry to Computer: The Pattern of Military Revolutions', *The National Interest*, 1994, p. 30, https://nationalinterest.org/article/cavalry-to-computer-the-pattern-of-military-revolutions-848.

10 Tai Ming Cheung, 'A conceptual framework of defence innovation', *Journal of Strategic Studies*, June 2021, https://www.tandfonline.com/doi/full/10.1080/01402390.2021.1939689.

11 F. R. Baumgartner and B. D. Jones, *Agendas and Instability in American Politics* (Chicago: University of Chicago Press, 2010); C. E. Lindblom, 'The science of "muddling through"', *Public Administration Review*, vol. 19, no. 2, 1959, pp. 79–88.

12 I. Porche, C. Paul, C. Serena, C. Clarke, E. Johnson and D. Herrick, *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*, RAND Corporation, 2017, https://www.rand.org/pubs/research_reports/RR1600.html.

13 On such adaptations, see T. Farrell, 'Improving in war: Military adaptation and the British in Helmand Province, Afghanistan, 2006–2009', *The Journal of Strategic Studies*, vol. 33, no. 4, 2010, pp. 567–94. On military transformation, see Krepinevich, 'Cavalry to computer'; S. P. Rosen, *Winning the next war* (Ithaca, NY: Cornell University Press, 2018); T. Farrell, T. Terry, and O. Frans (eds.), *A transformation gap?: American innovations and European military change* (Palo Alto, CA: Stanford University Press, 2010).

14 On the diffusion of cyber forces, see Jason Blessing, 'The Global Spread of Cyber Forces, 2000–2018', 13th International Conference on Cyber Conflict, May 2021. On temporal dynamics, which are prevalent in the military diffusion literature, see M. C. Horowitz, *The Diffusion of Military Power* (Princeton, NJ: Princeton University Press, 2010).

15 On the methodological consequences of timing and sequencing, see J. Mahoney, 'Process tracing and historical explanation', *Security Studies*, vol. 24, no. 2, 2015, pp. 200–218; J. Mahoney, K. Mohamedali and C. Nguyen, 'Causality and time in historical institutionalism', *The Oxford Handbook of Historical Institutionalism* (Oxford: Oxford University Press, 2016), pp. 71–88.

16 See the brief discussion of 'operational experience' in Appendix 1.

17 Our judgement comes with a caveat that the public evidence for such a judgement is far from comprehensive, but our judgement is also informed by non-public sources.

18 C. Stephen Carr, Stephen D. Crocker and Vinton G. Cerf, 'HOST-HOST Communication Protocol in the ARPA Network', Advanced Research projects Agency, 12 February 1970, https://datatracker.ietf.org/doc/html/rfc33.

19 Craig Wiener, 'Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation', PhD dissertation, 2016.

20 Cyber Command website, https://www.cybercom.mil/About/History/.

21 Statement of General Paul M. Nakasone, Commander United States Cyberspace Command, before the 117th Congress Senate Armed Services Committee 25 March 2021, p.1, https://misi.tech/docs/Nakasone_03-25-21.pdf.

22 Martin Matashak, 'House defense policy bill okays $10.4 billion for DoD cybersecurity', The Record, 30 August 2021, https://therecord.media/house-defense-policy-bill-okays-10-4-billion-for-dod-cybersecurity/.

23 Key doctrine statements include Joint Chiefs of Staff, 'Cyberspace Operations', 2018, Joint Publication 3–12, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf; Joint Chiefs of Staff, 'Information Operations', 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf. Key policy documents include DoD, 'Summary: Department of Defense Cyber Strategy', 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

24 Cyber Command, 'Beyond the Build: Delivering Outcomes through Cyberspace', Department of Defense, 2015, https://dod.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf.

25 Cyber Command, 'Beyond the Build: Delivering Outcomes through Cyberspace', Department of Defense, 2015, https://dod.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf.

26 See IISS, 'Cyber Capabilities and National Power: Methodology and Net Assessment'.

27 There are significant innovations in the 2015 policy statements from the Pentagon, including recognition in 'Beyond the Build' that cyber defences in DoD are weaker than the threats it faces and that military units must be able to operate with degraded systems and a lack of cyber situational awareness (including command and control, intelligence and targeting data).

28 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.

29 Admiral Phillip S. Davidson, 'Transforming the Joint Force: A Warfighting Concept for Great Power Competition', San Diego CA, 3 March 2020, https://www.pacom.mil/Media/Speeches-Testimony/Article/2101115/transforming-the-joint-force-a-warfighting-concept-for-great-power-competition/.

30 Joseph S. Nye Jr and and William A. Owens, 'America's information edge', *Foreign Affairs*, vol. 75, 1996, pp. 20–36.

31 Christopher Paul, Colin P. Clarke, Bonnie L. Triezenberg, David Manheim and Bradley Wilson, 'Improving C2 and Situational Awareness for Operations in and through the Information Environment', Rand, 2018, p. xiii, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2400/RR2489/RAND_RR2489.pdf.

32 The Rand report mapped out several pathways to a full transformation in the paradigm of warfighting.

33 John R. Bolton, *The Room Where It Happened: A White House Memoir* (New York: Simon and Schuster, 2020), p. 175.

34 US Senate Armed Services Committee, Stenographic Transcript Before the Committee on Armed Services US Senate Nominations for Lieutenant General Paul Nakasone to be Commander of the US Cyber Command and Director of the National Security Agency and Chief of the Central Security Service, 1 March 2018, p. 52, unclassified., https://nsarchive2.gwu.edu/dc.html?doc=4407097-United-States-Senate-Armed-Services-Committee.

35 United States Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command', 2018, p. 7, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf. This task of integration was identified as one of five priorities for Cyber Command.

36 Richard G. Hewlett and Francis Duncan, *Nuclear navy, 1946–1962*, Atomic Energy Commission, 1974, p. 51, https://www.osti.gov/servlets/purl/4268624.

37 Ernest R. May, John D. Steinbrenner, and Thomas W. Wolf, 'History of the Strategic Arms Competition 1945–1972', Washington, 1981, available at the National Security Archive, Washington DC.

38 Miguel Alberto N. Gomez, 'Sound the alarm! Updating beliefs and degradative cyber operations', *European Journal of International Security*, vol. 4, no. 2, 20 March 2019, p. 193. This is Gomez's overview of the main trend in the scholarly literature.

39 Admiral Phillip S. Davidson, 'Transforming the Joint Force: A Warfighting Concept for Great Power Competition', San Diego CA, 3 March 2020, https://www.pacom.mil/Media/Speeches-Testimony/Article/2101115/transforming-the-joint-force-a-warfighting-concept-for-great-power-competition/.

40 The US cyber attack against the Belgrade electric grid in 1999 is debated among scholars but there is considerable evidence for it, including undocumented personal reflections by senior officers who led the operation. The most compelling piece of public evidence is a statement by the NATO spokesman,

Jamie Shea, during the bombing: 'The fact that lights went out across 70 percent of the country shows that NATO has its finger on the light switch now… We can turn the power off whenever we need to and whenever we want to'. Michael A. Gordon, 'Crisis in the Balkans: The Overview; NATO Air Attacks on Power Plants Pass a Threshold', *New York Times*, 4 May 1999, https://www.nytimes.com/1999/05/04/world/crisis-balkans-overview-nato-air-attacks-power-plants-pass-threshold.html. At the time, the electric grid was managed with portable logic controllers in Siemens equipment that had no security. See also B. Lambeth, 'NATO's Air War for Kosovo: A Strategic and Operational Assessment', Rand 2001, p. 112, https://www.rand.org/pubs/monograph_reports/MR1365.html. Lambeth discusses other cyber offensive operations against military systems in the Kosovo campaign, citing US officials.

41 C. Todd Lopez, 'Commander Discusses a Decade of DOD Cyber Power', DoD News, 21 May 2020, https://www.defense.gov/News/News-Stories/Article/Article/2193130/commander-discusses-a-decade-of-dod-cyber-power/.

42 Africa Command, Central Command, Cyber Command, European Command, Indo-Pacific Command, Northern Command, Southern Command, Space Command, Cyber Command, Special Operations Command and Transportation Command.

43 IISS, *Cyber Capabilities and National Power: A Net Assessment*, pp. 93–4, p. 174.

44 Jiang Zemin, *On the Development of China's Information Technology Industry*, translated, (Elsevier, Oxford: Central Party Literature Press and Shanghai Jiaotong University Press, 2010) (first published in Chinese in 2009).

45 See Greg Austin, *Cyber Policy in China*, Polity Press, Cambridge, 2014, pp. 130–6 for the period 2000 to 2010.

46 *Ibid.*, pp. 136–45 for the years to 2014.

47 See Xi Jinping, 'Speech at the Work Conference for Cybersecurity and Informatization', translated in China Copyright and Media, 19 April 2016, https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/.

48 Masha Borak, 'China drafts three-year plan to boost its cybersecurity industry amid increasing concerns for data safety', South China Morning Post, 14 July 2021, https://www.scmp.com/tech/policy/article/3140963/china-drafts-three-year-plan-boost-its-cybersecurity-industry-amid#:~:text=Last%20year%2C%20the%20MIIT%20said%20that%20China%E2%80%99s%20cybersecurity,the%20highest%20growth%20expected%20in%20the%20Asia-Pacific%20region.

49 See Rebecca Slayton, 'What Is a Cyber Warrior? The Emergence of US Military Cyber Expertise, 1967–2018, *Texas National Security Review*, vol. 4, no. 1, pp. 62–96, https://tnsr.org/2021/01/what-is-a-cyber-warrior-the-emergence-of-u-s-military-cyber-expertise-1967-2018/.

50 See Greg Austin, 'Strategic Implications of China's Weak Cyber Defences', *Survival*, vol. 62, no. 5, pp. 119–38, https://www.tandfonline.com/doi/abs/10.1080/00396338.2020.1819648?journalCode= tsur20; and Greg Austin and Wenze Lu, 'Five Years of Cyber Security Education in China; in Greg Austin (ed.), *Cyber Security Education: Policies and Principles*, (Abingdon: Routledge, 2020), pp. 173–93.

51 Roderick Lee, 'Building the Next Generation of Chinese Military Leaders', *Journal of Indo-Pacific Affairs*, Fall, 2020, pp. 135–42, https://media.defense.gov/2020/Aug/31/2002488091/-1/-1/1/LEE.PDF.

52 See Anil Chopra, 'People's Liberation Army Strategic Support Force – A Comprehensive Look', Air Power Asia, 8 March 2021, https://airpowerasia.com/2021/03/08/peoples-liberation-army-strategic-support-force-a-comprehensive-look/.

53 Greg Austin, Munish Sharma and Kai Lin Tay, 'Great Power Offensive Cyber Campaigns: Experiments in Strategy', forthcoming.

54 Australian Government – Department of Defence, 'Future Joint Operating Concept 2030', March 2011, p. 8.

55 Colin Cosier, 'Serious cyber attack has potential to cause same damage as terrorist attack', Dan Tehan says', ABC News, 23 November 2016, https://www.abc.net.au/news/2016-11-23/cyber-attack-potential-cause-same-damage-terrorist-attack/8051716\.

56 Malcolm Turnbull, 'Australia and the US: New Responsibilities for an Enduring Partnership', Remarks at CSIS, 18 January 2016, https://pmtranscripts.pmc.gov.au/release/transcript-40161.

57 Cosier, 'Serious Cyber Attack'.

58 Marcus Thompson, 'Harmonised Taxonomies of Security and Resilience: A Suitable Foundation for the Security Discipline', Public Version, PhD Dissertation, University of New Wales Canberra, 2016, available through http://unsworks.unsw.edu.au/fapi/datastream/unsworks:38393/SOURCE01?view=true.

59 Ministry of Defence, 'Cyber Security Strategy', Cyber Security Strategy Committee, Ministry of Defence, 2008, https://www.

enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en.

60 Ministry of Economic Affairs and Communication, *2014–2017 Cyber Security Strategy*, 2014, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf.

61 NATO Cooperative Cyber Defence Centre of Excellence, 'Centre Contributed to New Estonian Cyber Security Strategy', 29 December 2014, https://ccdcoe.org/news/2014/centre-contributed-to-the-new-estonian-cyber-security-strategy/.

62 Estonian Defence Forces, 'Terras: NATO Kavandab Eestisse Küberharjutusvälja Loomist' [Terras: NATO Plans to Create a Cyber Training Range in Estonia], 12 June 2014, https://mil.ee/uudised/terras-nato-kavandab-eestisse-kuberharjutusvalja-loomist/.

63 Jason Blessing, 'The Diffusion of Cyber Forces: Military Innovation and the Dynamic Implementation of Cyber Force Structure', Doctoral dissertation Syracuse University, 2020, p. 216, https://surface.syr.edu/etd/1190/

64 The other members are the US, the UK, the Netherlands, and Denmark; https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/.

65 S. Sprenger, 'Estonia, US launch effort to ease sharing of cyberthreat intel', Fifth Domain, 17 January 2020, https://www.fifthdomain.com/global/europe/2020/01/17/estonia-us-launch-effort-to-ease-sharing-of-cyberthreat-intel/.

66 US Cyber Command, 'Hunt Forward Estonia: Estonia, US strengthen partnership in cyber domain with joint operation', 2020, https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/.

67 UK Ministry of Defence, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review,* 2010, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf.

68 A. Chuter and A. Mehta, 'How the UK's Joint Forces Command is about to change — and why it won't be easy', DefenseNews, 26 April 2019, https://www.defensenews.com/global/europe/2019/04/25/how-the-uks-joint-forces-command-is-about-to-change-and-why-it-wont-be-easy/.

69 HMG, 'Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012–13 – Defence Committee', 22 March 2013, https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/719/71904.htm; A. Osula, 'National Cyber Security Organisation: United Kingdom', NATO CCDCOE, 2015, https://ccdcoe.org/uploads/2018/10/CS_organisation_UK_032015_0.pdf.

70 J. Blitz, 'UK becomes first state to admit to offensive cyber attack capability', *Financial Times*, 2021, https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de\.

71 R. Chesney, 'Adapting to the Cyber Domain: Comparing Us and UK Institutional, Legal, and Policy Innovations', Hoover Institution, Aegis Series Paper No. 2103, 2021, https://www.hoover.org/sites/default/files/research/docs/chesney_webreadypdf_0.pdf.

72 *Ibid*., p. 40; HMG, *National Security Strategy and Strategic Defence Security Review 2015: A Secure and Prosperous UK,* 2015, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf.

73 Chesney, 'Adapting to the Cyber Domain', pp. 24–25.

74 M. Fallon, 'Defence Secretary's speech at the second RUSI Cyber Symposium', 21 October 2016, https://www.gov.uk/government/speeches/defence-secretarys-speech-at-the-second-rusi-cyber-symposium.

75 M. Fallon, 'Defence Secretary's speech at Cyber 2017 Chatham House Conference'. 27 June 2017, https://www.gov.uk/government/speeches/defence-secretarys-speech-at-cyber-2017-chatham-house-conference.

76 J. Devany, A. Dwyer, A. Ertan and T. Stevens, 'The National Cyber Force that Britain Needs?', King's College London, April, 2021, https://www.kcl.ac.uk/policy-institute/assets/the-national-cyber-force-that-britain-needs.pdf.

77 D. Haynes, 'Britain to create 2,000-strong cyber force to tackle Russia threat', Sky News, 21 September 2018, https://news.sky.com/story/britain-to-create-2000-strong-cyber-force-to-tackle-russia-threat-11503653; Lucy Fisher, 'Britain steps up cyber offensive with new £250m unit to take on Russia and terrorists', *The Telegraph*, 21 September 2018, https://www.telegraph.co.uk/news/2018/09/21/britain-steps-cyber-offensive-new-250m-unit-take-russia-terrorists/.

78 M. Willett, 'Why the UK's National Cyber Force is an important step forward', IISS, 20 November 2020, https://www.iiss.org/blogs/analysis/2020/11/uk-national-cyber-force.

79 Chesney, 'Adapting to the Cyber Domain', p. 25.

80 P. Mordaunt, 'Defence Secretary keynote speech at the Air and Space Power Conference 2019', 18 July 2019, https://

www.gov.uk/government/speeches/defence-secretary-keynote-speech-at-the-air-and-space-power-conference-2019.

81 G. Corera, 'UK's National Cyber Force comes out of the shadows', BBC News, 20 November 2020, https://www.bbc.co.uk/news/technology-55007946.

82 Chesney, 'Adapting to the Cyber Domain', pp. 20, 27.

83 Judah Ari Gross, 'Army beefs up cyberdefense unit as it gives up idea of unified cyber command,' *The Times of Israel*, 14 February 2017, https://www.timesofisrael.com/army-beefs-up-cyberdefense-unit-as-it-gives-up-idea-of-unified-cybercommand/; Gabi Siboni and Ofer Assaf, 'Guidelines for a national cyber strategy', Tel Aviv: Institute for National Security Studies, 2016, p. 58, https://www.inss.org.il/wpcontent/uploads/systemfiles/INSS%20Memorandum%20153%20-%20Guidelines%20for%20a%20National%20Cyber%20Strategy.pdf

84 IISS, ' Capabilities and National Power: A Net Assessment', p. 74

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

86 IISS, Cyber Capabilities and National Power: A Net Assessment, p. 71.

87 D. Fulghum and D. Barrie, 'Israel used electronic attack in air strike against Syrian mystery target', ABC News, 9 October 2007, https://abcnews.go.com/Technology/story?id=3702807&page=1.

88 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; David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, (New York: Broadway Books, 2018), p. 25; 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; Lior Tabansky, 'Israel Defense Forces and National Cyber Defense', *Connections*, vol. 19, no. 1, 2020, p. 56; Y. Katz, 'IDF admits to using cyber space to attack enemies', *The Jerusalem Post*, 3 June 2012, https://www.jpost.com/Defense/IDF-admits-to-using-cyber-space-to-attack-enemies.

89 N. Perlroth, 'Researchers Find Clues in Malware', *The New York Times*, https://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html; K. Zetter, 'Meet "Flame", The Massive Spy Malware Infiltrating Iranian Computers', *Wired Magazine*, 28 May 2012, https://www.wired.com/2012/05/flame/; E. Nakashima, G. Miller and J. Tate, 'US, Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say', *The Washington Post*, 19 June 2012, https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

90 B. Opall-Rome, 'Israel Begins Modernisation Plan through 2030', DefenseNews, 24 January 2017, https://www.defensenews.com/global/mideast-africa/2017/01/23/israel-begins-modernisation-plan-through-2030/.

91 Seth J. Frantzman, 'Israel Rolls Out New Wartime Plan to Reform Armed Forces', DefenseNews, 18 February 2020, https://www.defensenews.com/global/mideast-africa/2020/02/18/israel-rolls-out-new-wartime-plan-to-reform-armed-forces/.

92 Tabansky, 'Israel Defense Forces and National Cyber Defense'.

93 J. Frei, 'Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organisations', ETH Zürich, 2020, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf.

94 S. Herpig, R. Morgus and A. Sheniak, 'Active Cyber Defense-A comparative study on US, Israeli and German approaches', Konrad Adenauer Stiftung, March 2020, p. 7, https://www.kas.de/documents/263458/263507/Active+Cyber+Defense+-+A+comparative+study+on+US,+Israeli+and+German+approaches.pdf.

95 'IDF Scraps Plans for a Unified Cyber Command', Israel Defense, 31 October 2017, https://www.israeldefense.co.il/en/node/29613.

96 Behar Richard, 'Inside Israel's Secret Startup Machine,' Forbes, 11 May 2016. https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/

97 Dmitry Adamsky, 'The Israeli Odyssey towards its National Cyber Security Strategy', *The Washington Quarterly*, 2017, vol. 40, no. 2, p. 120.

98 Frei, 'Israel's National Cybersecurity and Cyberdefense Posture', p. 8.

99 Gil Baram and Kevjn Lim, 'Israel and Iran Just Showed Us the Future of Cyberwar with Their Unusual Attacks'. Foreign Policy, 5 June 2020, https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-

their-unusual-attacks/; '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

100 IISS, 'Cyber Capabilities and National Power: A Net Assessment', p. 71; Behar, 'Inside Israel's Secret Startup Machine'; Seth Adler, 'Inside the Elite Israeli Military Unit 8200', https://www.cshub.com/threat-defense/articles/inside-the-elite-israeli-military-unit-8200.

101 Y. Bob, 'Eisenkot: Someday the IDF will be under one cyber command', *The Jerusalem Post*, 24 October 2018, https://www.jpost.com/Israel-News/Eisenkot-Someday-the-IDF-will-be-under-one-cyber-command-570230.

102 Israel National News, 'Who is Major General Aviv Kochavi?' 26 October 2018, https://www.israelnationalnews.com/News/News.aspx/253822.

103 Doctrine, organisation, training, personnel, leadership, facilities, and interoperability. Neil Robinson, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, Pablo Rodriguez, 'Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP) ', Unclassified Summary, 2013, https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR286/RAND_RR286.pdf.

104 Max Smeets, 'NATO members' Organisational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis', in T. Minarik et al. (eds.) *2019 11th International Conference on Cyber Conflict: Silent Battle*, Tallinn, Estonia: NATO CCD COE, 2019, https://ccdcoe.org/uploads/2019/06/Art_09_NATO-Members-Organisational-Path.pdf.

105 Blessing, 'The Diffusion of Cyber Forces'. Jason Blessing, 'The Global Spread of Cyber Forces, 2000–2018' In T. Jančárková et al. (eds.), 2021 13th International Conference on Cyber Conflict, Tallinn, Estonia: NATO CCDCOE Publications, 2021, 233–55.

106 David Ormrod and Benjamin Turnbull, 'The Military Cyber-Maturity Model: Preparing Modern Cyber-Enabled Military Forces for Future Conflicts, 11th International Conference on Cyber Warfare and Security: *ICCWS2016,* 2016.

107 R. Brooks, 'Technology and Future War Will Test US Civil–Military Relations', War on the Rocks, 26 November 2018, https://warontherocks.com/2018/11/technology-and-future-war-will-test-u-s-civil-military-relations/.

108 IISS, 'Cyber Capabilities and National Power: A Net Assessment', 28 June 2021, p. 9.

109 R. Brooks, *Shaping Strategy*, (Princeton, NJ: Princeton University Press, 2008).

110 A. Arslaner and P. Voyatzakis, 'Institution Building and Cyberwarfare Capabilities in China: A Study of Doctrine and Civil Military Relations', undated, https://www.northcom.mil/Portals/28/ArslanerVoyatzakisFinalwDisclaimer.pdf?ver=tb3w_QLtcryI7ylqqBYenQ%3D%3D.

111 Sergei Boeke, Matthijs A. Veenendaal, and Caitriona H. Heinl, 'Civil–Military Relations and International Military Cooperation in Cyber Security: Common Challenges and State Practices across Asia and Europe,' in 7th International Conference on Cyber Conflict (Architectures in Cyberspace), Tallinn, Estonia: NATO CCD COE Publications, 2015, p. 75.

112 M. Smeets, 'US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection', *Intelligence and National Security*, vol. 35, no. 3, 2020, pp. 444–53.

113 This is not unique to the cyber domain. For example, the operational experiences of US submarine forces during World War II provided important feedback on the strategic payoff of targeting Japanese merchant ships. Rosen, *Winning the Next War: Innovation and the Modern Military*, pp. 52, 128, 132.

114 N. Kostyuk and Y. M. Zhukov, 'Invisible digital front: Can cyber attacks shape battlefield events?' *Journal of Conflict Resolution*, vol. 63, no. 2, 2019, pp. 317–47.

115 B. Valeriano, B. Jensen, and R. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018).

116 For examples, see Maral Mahdad, Chiara Eleonora De Marco, Andrea Piccaluga and lberto Di Minin, 'Harnessing adaptive capacity to close the pandora's box of open innovation', *Industry and Innovation*, 2019, 264–84.

117 S. Starr, D. Kuehl, and T. Pudas, 'Perspectives on building a cyber force structure', in C. Czosseck and K. Podins (eds.), Proc. Conf. on Cyber Conflict, CCD COE Publications, Tallinn, Estonia, 2010, 163–81, p. 170, https://ccdcoe.org/uploads/2018/10/Starr-Perspectives-on-Building-a-Cyber-Force-Structure.pdf.

118 S. P. White, *Subcultural influence on military innovation: The development of US military cyber doctrine*, Doctoral dissertation, Harvard University, 2019, https://dash.harvard.edu/handle/1/42013038.

119 Jacquelyn Schneider, 'Deterrence in and through Cyberspace' in Erik Gartzke and Jon Lindsay (eds.), *Cross-Domain*

Deterrence: Strategy in an Era of Complexity (Oxford: Oxford University Press, 2019), p. 120.

120 Boeke et al., 'Civil-Military Relations', pp. 74, 79.

121 M. Leed, 'Offensive Cyber Capabilities at the Operational Level: The Way Ahead', CSIS, 2013, https://www.csis.org/analysis/offensive-cyber-capabilities-operational-level.

122 Blessing *The Diffusion of Cyber Forces*.

123 *Ibid*.

124 Ormrod and Turnbull, 'The Military Cyber-Maturity Model'.

125 H. Lin, 'Oft-Neglected Cost Drivers of Cyber Weapons', Council on Foreign Relations, 2016, https://www.cfr.org/blog/oft-neglected-cost-drivers-cyber-weapons.

126 *Ibid*.

127 Max Smeets, 'How Much Does a Cyber Weapon Cost? Nobody Knows', Council on Foreign Relations, 2016, https://www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows.

128 Max Smeets, 'A Matter of Time: On the Transitory Nature of Cyberweapons', *Journal of Strategic Studies*, vol. 41, no. 1–2, 2018, pp. 6–32.

129 Leed, 'Offensive Cyber Capabilities'.

130 Starr et al., 'Perspectives on building a cyber force structure', p. 170.

131 Leed, 'Offensive Cyber Capabilities'.

132 Jacquelyn Schneider, 'Blue Hair in the Gray Zone', War on the Rocks, 10 January 2018, https://warontherocks.com/2018/01/blue-hair-gray-zone/.

Acknowledgements

IISS–Europe acknowledges the financial support of the German Federal Foreign Office in producing this research paper, including for a workshop that helped inform the paper's contents.

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