RESEARCH REPORT

THE STRATEGIC AND SYMBOLIC VALUE OF DIGITAL TECHNOLOGIES

AUTHORS
Max Smeets, James Shires, and Jakob Bund

July 2024

ECCRI EUROPEAN CYBER CONFLICT RESEARCH INITIATIVE

Executive summary

This report explores the nature and characteristics of digital technologies that states associate with strategic value. Combining conceptual and applied perspectives, the report develops guidance for navigating the opportunities and challenges presented by digital technological transformations and for fostering effective multilateral cooperation in this domain.

This report makes three key contributions:

- A framework for understanding strategic digital technologies: Building on existing conceptions of strategic assets, the report develops a framework specifically designed to capture the strategic properties of digital technologies. While acknowledging the context-dependent and evolving nature of strategic value, the framework highlights distinct dynamics around i) interoperability and standardization, ii) network effects, and iii) capability and control, which together contribute to the strategic value of digital technologies.

- An assessment of the strategic value for key digital technologies: The report uses the framework above to assess the strategic value of six digital technological fields and the organizational and social configurations required for and directly shaped by their deployment. These technologies are Artificial Intelligence (AI), Cybersecurity, Quantum Technologies, 5G, Internet of Things (IoT), and Cloud Computing. The resulting analysis of areas of shared and diverging strategic value facilitates further study of the ways and means by which states engage in the multilateral governance of these technologies.

- A comparative analysis of multilateral and national approaches to strategic digital technologies: To unpack the economic and societal factors that shape how states view the strategic qualities of technology, the report conducts a comprehensive review of how states engage on technology, both at the level of national strategies and as part of multilateral consultations, specifically in the framework of the UN Global Digital Compact (GDC).

These contributions facilitate further study of how the strategic value of digital technologies shapes multilateral engagement through its origin in and influence on the interests and beliefs of states and other actors. The comprehensive understanding of what makes certain digital technologies 'strategic' provides the first building blocks for a theory about the conditions that support substantial multilateral engagement.

Table of contents

Introduction

This report provides an overview of the nature of strategic digital technologies and their critical role in shaping global affairs. The findings and insights presented here are paving the way for subsequent in-depth studies that will further explain the interaction between digital technologies and global affairs.[1]

The report is structured into three sections. Section 1 explores what makes certain digital technologies 'strategic'. Our starting point for analysis is the framework by Ding and Dafoe, which assesses strategic value based on i) importance, ii) externality, and iii) nationalization. We then expand this framework to focus on the particular characteristics of digital technologies, identifying further factors in strategic value of iv) interoperability and standards, v) network effects, and vi) capability and control. These additional dimensions demonstrate how the strategic nature of digital technologies is significantly different to other kinds of technology or assets more broadly; and, moreover, that the strategic value of digital technologies is relative to state characteristics and priorities. Consequently, there is no such thing as strategic digital technologies per se - rather, specific digital technologies offer different strategic value to different states, at times contrasting, complementing and contradicting. The framework, which facilitates the coherent analysis of these differences in state approaches, aims to identify the main characteristics and trends in strategic digital technologies.

Section 2 builds on this insight by providing an analysis of the types and properties of some of the key strategic digital technologies: artificial intelligence (AI), cybersecurity, quantum technologies, 5G, the internet of things (IoT), and cloud computing. This illustrative list of technologies has been chosen to align with the focus of future case studies. The list is, however, far from exhaustive. Some technologies, such as semiconductors, are foundational to the development of digital technologies overall: they represent both an integral part of each field above, and a distinct focus of technological innovation, policy, and strategy; we have chosen to emphasize the former aspect. Other technologies, such as blockchain, offer perhaps more radical challenges to the assumptions of state control and strategic value detailed here; however, those theoretical challenges have so far not been fully realised in practice, and such technologies would therefore be a worthy addition to the list examined here.

We assess the strategic value of each technological field - encompassing both the technologies involved and the organizational and social configurations required for and directly shaped by their deployment - via the six factors above. Despite the relativity of strategic value, this section nonetheless identifies different themes in the strategic value of each technological field: AI's widespread applications and spillover effects, quantum computing's transformative potential in cryptography, cybersecurity's crucial role in national security, 5G's significance in communication and economic impact, IoT's expansive connectivity, and the vast data processing power enabled by cloud computing. These findings contribute to a greater understanding of the strategic properties and implications of digital technologies overall.

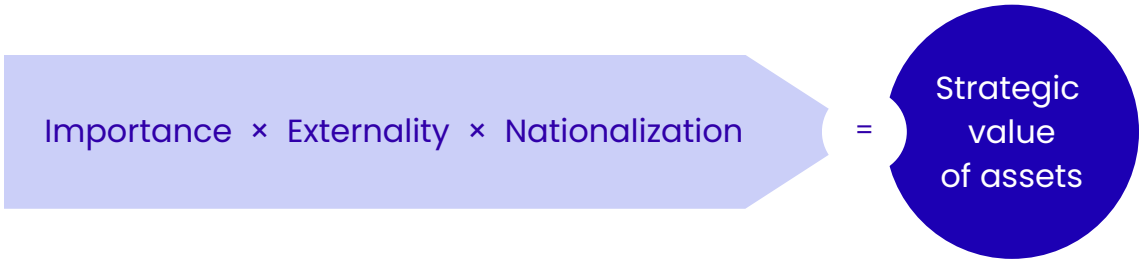
Section 3 offers an overview of the global political debate over strategic digital technologies. It applies the framework of Section 1 to two sets of state documents: first, state submissions to consultations for the UN Global Digital Compact (GDC); and, second, national technology strategies.

Despite its limitations within the UN system, and broader questions over the relevance of UN processes for digital technology governance, the GDC nonetheless has high ambitions: to provide a platform for comprehensive dialogue about technological potential and possible related harm at a global level. Whatever their ultimate policy impact, GDC consultations raise a broad spectrum of economic and societal implications presented by digital technologies, and therefore offer a useful window into states' perspectives on the strategic value of digital technologies. This overview demonstrates how the framework for understanding strategic value presented here can facilitate the identification of viable initiatives and potential fault lines for multilateral engagement.

1. What makes digital technologies 'strategic'?

This first part of this report examines the factors that render digital technologies strategic. Echoing Baldwin's observation from years ago, the misunderstanding of 'strategic goods' continues to hinder meaningful discourse in governance.[2] Addressing this issue, Ding and Dafoe propose a framework to better understand strategic assets.[3] Although there are of course many potential frameworks for thinking about the relationship of technology to strategy, this framework stands out because it combines versatility with flexibility.[4] Its broad scope provides for continuity in analysing how digital technology compares to other strategic assets.

At the same time, it is open to expansion, allowing for the integration of additional factors to account for properties specific to digital technologies. Its recent publication means that it already considers many of the strategic questions raised by digital technologies -for example, Ding and Dafoe explore applying the framework to AI and point out its relevance for telecommunications technology and chips[5] - and the framework explicitly invites future research to further develop its applicability.[6] The second half of this section introduces three such complementing factors. In the original format, Ding and Dafoe contend that three principal factors determine an asset's strategic value:



Strategic value of assets

Importance: This refers to the economic, military, or security value of an asset. Certain sectors, like freight transport, have a more significant impact on economic growth compared to others, like fashion or gaming.

Externality: This involves the economic, military or security impacts that extend beyond the immediate use of the asset. Often, private firms and military organizations fail to fully address these externalities. For instance, private entities might underinvest in foundational technology research due to not benefiting from all its indirect advantages.

Nationalization: This measures how much the externalities of an asset become competitive points between countries. For example, breakthroughs in fundamental medical research might benefit multiple countries, thereby reducing the strategic advantage for any one nation.

Ding and Dafoe's framework serves as a useful starting point for understanding the strategic value of assets, including digital technologies. A key advantage is its clarity and structure, providing a tangible set of criteria to evaluate an asset's strategic value. It also goes further, linking these three factors in turn to three distinct logics: cumulative (strategic value increases with greater possession of relevant assets); infrastructure (strategic value increases with the wider role of relevant assets in underpinning other fields); and dependency (strategic value increases the scarcer and more reliant others are on those assets). While we refer to these logics below where relevant, we focus primarily on the three factors above, as these are more appropriate for the purposes of this report in understanding the sources of strategic value for digital technologies. Later work, considering the dynamics of individual technologies through case studies, may rely more on the logics than the underlying factors themselves.

This framework also has several disadvantages for our purposes. First, one could differentiate more clearly between short-term and long-term strategic value. Some assets may have immediate strategic importance due to current geopolitical or economic conditions, while others gain strategic value over a longer period. Second, the framework may oversimplify the nuanced interplay between economic, military, and security factors, treating them as alternative sources of value rather than as interacting and overlapping - and sometimes competing - areas contributing to an overall assessment of an asset's value.

Most importantly, Ding and Defoe explicitly develop their framework to address strategic assets in general, rather than technological assets specifically. Of course, technologies do not exist in a vacuum, hence we use the term "technologies" as shorthand for technological fields, encompassing both the technologies involved and the organizational

and social configurations required for and directly shaped by their deployment. Even so, applying this framework to technologies - especially digital technologies[7] - requires closer attention to their affordances: in other words, what kinds of activities they make possible or more likely, and where they introduce friction or resistance for other actors.

Consequently, when applying Ding and Dafoe's framework specifically to strategic digital technologies as a subset of strategic assets, we argue that several additional considerations contribute to a more granular understanding of strategic value for this particular subcategory of assets.[8] We draw these three considerations from the wider literature on digital technologies, especially software, computing, and internet governance, which highlights these considerations as key markers of difference between digital technologies and other technological fields.

The first is interoperability and standards. The strategic value of digital technologies is influenced by their compatibility and standardization across different platforms and countries. Digital technologies that set or adhere to international standards may have increased strategic value due to their widespread applicability and potential for creating dependencies.[9] This includes Wi-Fi standards like IEEE 802.11 that are globally recognized and facilitate compatibility across devices and networks worldwide,[10] or the standardization of HTML and other web technologies that are crucial for the functionality of the internet.[11]

Around 55% of ICT standards are based on patents,[12] positioning holding companies to establish a central market position and earning them continuous licensing fees. The revenue and head-start to secure market share promised by patents, opens standardization to rent-seeking strategies and attempts to leverage standardization for corporate dominance. On the other hand, many digital technologies are based on open-source standards and code, remaining interoperable – and, arguably, insecure - precisely because the open-source model prevents direct corporate capture and encourages voluntary contributions.[13] While standardization is of course far broader than the digital realm, the fast pace of digital technological development generates frequent changes in standardization (both in terms of "churn", replacing old standards with new ones, and "stacking", causing new standards to rely on old ones). There is therefore strategic value in influencing or controlling standardization processes, organizations, and communities themselves, separate to the strategic value of the technologies they focus on at any specific time.

The second is network effects. Digital technologies often operate within ecosystems where the value of a single technology is vastly enhanced by the number of users and the connections between them.[14] This network effect can amplify a technology's strategic importance, as it becomes integral to a larger system of interconnected technologies.[15] The most popular examples are social media platforms. Platforms like Meta or Twitter become more valuable as more users join, creating a network where information can disseminate. Another example are E-commerce marketplaces like Amazon and Alibaba, as more sellers attract more buyers.

While Ding and Defoe would likely include network effects in their "cumulative logic" of strategic value, defining it as "a broad concept that covers long investment timelines, first-mover advantages, winner-take-all dynamics, learning by doing, etc.", we argue that - for digital technologies at least - network effects are so substantial that they deserve separate analysis as a factor for strategic value.

The third aspect in assessing the strategic value of digital technology is capability and control.[16] This factor goes beyond mere possession or usage; it encompasses who has the expertise to develop and maintain it, and who governs its distribution and access.[17] In this sense, capability and control captures both the ability to shape a technology throughout its life cycle as well as leverage over the access of other actors at each of node of the life cycle. An example are cloud services like Amazon Web Services and Microsoft Azure, as the strategic value of these platforms depends on who controls them: both who has the capability to exploit them (both commercially and adversarially), and who makes decisions around access and removal. Satellite networks, such as those owned by SpaceX (Starlink), also present new challenges of capability and control. In many analyses of strategic value, capability and control are primarily contested by and between states and intergovernmental entities. In contrast, relevant actors for digital technologies include not only states, but also private sector and other non-state actors, especially multinational technology companies such as those above.[18] Such actors can not only try to refuse to comply with state direction (whether their "home" or headquartered state or others), but develop new conceptualizations and practical implementations of their technologies that are unavailable to states. Apple's implementation of device-level encryption, for example, put access to iPhones beyond the control of Apple as manufacturer, introducing technical hurdles to executing decryption orders from law enforcement.[19]

A few further examples help to illustrate how these three aspects – interoperability and standards, network effects, and capability and control – contribute to the strategic value of digital technologies. In terms of standardization, regulations imposed by governments or international bodies can significantly impact the strategic value of a technology by either enhancing or limiting its deployment and development.[20]

Regulations like the European Union's General Data Protection Regulation (GDPR) have significantly impacted how companies have to handle personal data, affecting the strategic value of data-centric businesses. In terms of network effects, the uneven distribution of different social media platforms worldwide - and their implications for censorship, disinformation and information operations, and online safety - is largely due to network-based patterns of adoption and recommendation. Facebook's connections to political violence in Myanmar, or TikTok's reputational damage in the US and Europe, affect not just the companies themselves, but the course of domestic and regional politics. In terms of capability and control, ownership and usage patterns of technology can shift based on political relations, trade agreements, or security alliances.[21] For example, a country may prefer certain providers over others for its 5G network based on security alliances or geopolitical tensions.[22]

Furthermore, as states embrace strategic digital technologies, they confront a 'capability/vulnerability paradox'.[23] The digital technologies that enhance their capabilities also create new vulnerabilities. Essential military systems like mission planning software, undersea cables, and satellite links, vital for real-time strategic communication, become potential cyber threats.[24] This dynamic leads to a dual development strategy: while states develop digitally dependent military technologies, they simultaneously invest in offensive cyber capabilities to exploit vulnerabilities in advanced, digitized societies.[25] Digital advancement therefore inherently needs to be balanced with the need to mitigate cyber risks.[26] As technological breakthroughs have the possibility to support both cyber defence and offence, a decision to not adopt this potential, or a lack in ability to do so, poses a risk in its own right, for example when threat actors use generative AI to identify target-specific vulnerabilities and develop tailored exploitation techniques. Ultimately, the most vulnerable states are those that adopt new technologies (whether by choice or economic or military necessity), but are unable to invest sufficiently in protecting them.

> *"The symbolic value of digital technologies is reflected in hype cycles and technological "fashions" from AI governance to 5G security panics. In such events, states act not only according to economic and military imperatives, but from social pressures to conform and gain status in international society."*

Finally, the strategic value of digital technologies is a product of both their inherent characteristics and the socio-geopolitical environment in which they operate. More specifically, digital technologies have symbolic value as well as utility: they are important for what they communicate to others about their owner, possessor or user, as well as their actual application (the Mac user does not only believe their machine is more powerful or well-designed, but makes a statement about who they are). In international politics, the symbolic value of digital technologies can be most easily understood as their contribution to national identity, prestige, and self-image.[27]

Although not addressed by Ding and Dafoe, symbolic elements operate according to similar logics: states value them differently (importance); they are by definition externalities; and some symbolic properties (like cultural status, respect or superpower status) are to some degree rivalrous, as not every state can have it to the same extent.

The symbolic value of digital technologies is reflected in hype cycles and technological "fashions" from AI governance to 5G security panics. In such events, states act not only according to economic and military imperatives, but from social pressures to conform and gain status in international society. Consequently, the three additional considerations put forward here – interoperability and standardization, network effects, and capability and control - also contribute to the symbolic as well as the more direct strategic value of digital technologies. While the remainder of this report focuses on direct strategic value for several digital technologies, further research may evaluate the relative weight of strategic and symbolic value for specific technologies, including how the additional considerations put forward here contribute to symbolic value in specific cases.

2. The strategic value of specific digital technologies

This section of the report delves into the types and properties of particular strategic digital technologies. Although, as outlined above, digital technologies cannot be strategic in general, because their strategic value is relative to state choices and characteristics, we select six digital technologies - more accurately, digital technological fields - that appear frequently in current policy discourses. This list is therefore not exhaustive, nor static - the range and emphasis on the strategic value of particular digital technologies will change. For example, one could include blockchain, which stands out for its decentralization, transparency, and security.

As a distributed ledger technology, it offers a tamper-proof way of recording transactions, applicable in various sectors including finance, supply chain management, and secure voting systems. However, blockchain technologies are not yet, in our judgement, at the same level of strategic value as the others listed here. The six technologies are as follows, in no specific order:

Technology clusters

1. Artificial intelligence (AI): AI represents a significant shift in how data is processed and decisions are made.[28] Properties include the ability to learn from data, adapt to new information, and perform complex tasks with increasing accuracy over time. These technologies are pivotal in areas such as automated decision-making, predictive analytics, and pattern recognition, offering strategic advantages in both civilian and military applications.[29]

2. Cybersecurity: The ever-evolving landscape of cyber threats makes cybersecurity essential.[30] Key properties include robustness, adaptability, and the ability to detect and mitigate threats proactively. These technologies safeguard critical infrastructure and sensitive data, playing a strategic role in protecting national security and other information.

3. Quantum technologies: Quantum technologies encompass a wide range of sensing, communication, and computing technologies, with different stages of development and strategic relevance.[31] Quantum computing is characterized by its potential to perform calculations at speeds unachievable by classical computers. Properties, such as superposition and entanglement, enable the rapid solution of complex problems, which has far-reaching implications for fields like cryptography, material science, and drug discovery.[32] Underlying quantum principles facilitate extreme-precision sensing and fundamental changes to the (in)security of communications, including the possibility of breaking encryption algorithms. Yet, a key limitation of current quantum computing platforms has been the high error rate that is multiple orders of magnitude and several technological advances away from the level required to run a wider set of applications with the required level of stability.[33]

4. 5G and advanced communication technologies: 5G networks are defined by high data transmission speeds, reduced latency, and the ability to connect a vast number of devices simultaneously. This technology is crucial for enhancing communication capabilities, supporting IoT infrastructure, and enabling new applications such as autonomous vehicles and smart cities.[34] 6G is to push these advances in speed and reduced latency by making use of AI to increase the efficiency of communications.[35]

5. Internet of things (IoT): IoT is marked by its extensive connectivity, allowing everyday objects to collect and exchange data. This interconnectivity presents opportunities for increased efficiency and automation but also raises challenges related to security and data privacy.

6. Cloud computing: Finally, cloud computing has emerged as a key technology, characterized by its flexibility, scalability, and cost-efficiency. It enables on-demand access to computing resources like servers, storage, databases, and a wide range of application services over the internet.

We summarize the properties of each strategic digital technology above in Table 1 below, categorizing them according to Ding and Dafoe's conceptualization of strategic assets. Overall, the steps towards nationalization that we identify in the last column of Table 1 are all aspects of what might be called a move towards "technological sovereignty": imposing territorial limits or state power on emerging technologies.

In addition, Table 1 reveals intriguing contrasts between the different technologies. AI and quantum computing, for example, are both highly important, but their externalities and nationalization aspects differ.

AI's widespread application across economic and military sectors creates significant spillover effects in automation and decision-making, whereas quantum computing's potential impact is more concentrated in computing and cryptography, with distinct geopolitical implications.

> *Perhaps the outlier in this list is cybersecurity, which assumes a critical role in protecting all digital data and infrastructure, highlighting its direct impact on national security and underpinning many security concerns associated with other strategic technologies.*

5G is pivotal for enabling a wide array of new services, significantly impacting the economy and highlighting the importance of mobile infrastructure for national interest. It has become a key policy contention, underscoring differences in risk management strategies related to untrusted vendors.[36] This issue has spread to other technologies, leading to policies aimed at onshoring or nearshoring supply chains for AI and cloud services.

Perhaps the outlier in this list is cybersecurity, which assumes a critical role in protecting all digital data and infrastructure, highlighting its direct impact on national security and underpinning many security concerns associated with the other five technologies.[37]

Table 1: Strategic value properties, following Ding and Dafoe

	Importance	Externality	Nationalization
AI	High in both economic [38] and military [39] sectors	Spillover effects in automation, decision-making [40] Security	Rapid efforts to grow national AI industry base and regulate effects [41]
Cybersecurity	Crucial for protecting data and infrastructure [42]	Externalities affecting both public and private sectors [43]	Incorporated into top-tier national security strategies, "whole-of-society" approach [44]
Quantum technologies	Potential game-changer in computing and cryptography [45]	Advancements could lead to significant economic and security shifts [46]	Geopolitical implications in computing supremacy and value of encryption [47]
5G & Advanced communication technologies	Critical for communication and data transfer [48]	Enables new services, impacting economy broadly [49]	Sovereignty over population-level mobile communications and digital divide [50]
IoT	Essential for smart devices and automation [51]	Impacts on privacy, security, and efficiency across sectors [52]	States (and EU) introducing IoT regulation, forcing security measures on manufacturers [53]
Cloud computing	Fundamental for data storage, processing, and scalability [54]	Enables a wide range of services, but raises data sovereignty and security issues [55]	Data storage and processing across borders impacts national policy and security [56]

The additional properties contributing to strategic value proposed in this report - interoperability and standards, network effects, and capability and control - are listed by technology in Table 2 below. As with Table 1, the table is populated by summarizing the wider literature on each technology cited above. The table also presents interesting contrasts.

On the one hand, IoT demonstrates significant network effects, where its value escalates with increased data and device connectivity, highlighting the importance of widespread standardization.[57] On the other hand, quantum computing, still in its developmental phase,[58] exhibits more nascent network effects and a concentrated control by leading research institutions, reflecting its emerging nature. Concerns that insight into research progress may cede advantage to strategic competitors for a technology with strong first-mover benefits, for example through the breaking of conventional cryptography, add to the reasons for compartmentalization, at least during the initial phases of development. AI standardization is in its infancy, with several states taking distinct approaches to regulation amid unclear understanding of its main risks - systemic disruption from "frontier" AI, or more prosaic impacts on jobs and inequality.[59]

Cybersecurity, essential for data protection, relies heavily on widespread implementation of security standards and protocols,[60] such as Hypertext Transfer Protocol Secure (HTTPS) for the encryption of web traffic. Some of these security measures are open source, while others are proprietary or otherwise non-public. Yet, access to advanced cybersecurity tools varies, indicating a disparity in defensive capabilities across different entities.

5G technology, pivotal for modern communication networks, shows a strategic blend of infrastructural network effects and control that lies with telecom operators and governments,[61] underscoring its role in technological sovereignty (along with all the other technologies listed). Actors that lack direct capability and control over the underlying technology, such as states with a limited domestic industrial base or technology providers without full-stack implementations of 5G in their portfolio, may seek out other means to achieve control.[62] Initiatives like OpenRAN, as an alternative extension of communication networks that emphasizes interoperability between components of different manufacturers to reduce vendor dependency, aim to level out the difference in leverage between technology makers and technology users.[63]

"AI standardization is in its infancy, with several states taking distinct approaches to regulation amid unclear understanding of its main risks - systemic disruption from "frontier" AI, or more prosaic impacts on jobs and inequality."

Table 2: Additional strategic value properties

	Interoperability and standards	Network effects	Capability and control
AI	Nascent standards, with risk- based, sector-based, and safety-focused approaches [64]	Networking effects are similar to other digital technologies in terms of market capture and dominance [65]	Controlled by leading technology firms, debates over risks of open source [66]
Cybersecurity	Relies on universal security protocols and standards [67]	Wider adoption strengthens overall security posture [68]	Capacity for advanced cybersecurity protection varies [69]
Quantum technologies	Emerging standards in quantum algorithms and hardware [70]	Limited current network effect, but potential in scientific community	Controlled by leading companies, research institutions and countries [71]
5G & Advanced communication technologies	(Global) standards essential for device compatibility and network interoperability [72]	Network value grows with more users [73]	Control lies with telecom operators, cloud platforms and governments [74]
IoT	Standards critical for device communication and security [75]	Value increases with more connected devices [76]	Controlled by manufacturers, regulatory bodies [77]
Cloud computing	Standards for data storage, processing, and security arebcrucial [78]	Services become more valuable as more data and applications move to the cloud [79]	Controlled by major cloud service providers and subject to national regulations [80]

Finally, all six digital technologies have experienced shifts in their symbolic value over their lifetime so far. The starkest illustration of such shifts is AI, where repeated AI "winters" over the past half-century have been replaced with a sudden outpouring of interest, concern, and attention, generated by large language models (LLMs). While LLMs are only one sub-field of AI, their symbolic value in demonstrating the power of AI to be nearly human - or, at least, to generate human-like text, images, and videos - went far beyond what any experts had predicted. For states such as the UK, AI summits offered not just strategic value in shaping future regulation, but symbolic value in portraying them as technologically-minded, innovation-friendly locations.[81] Cybersecurity, on the other hand, has long been the subject of scepticism from practitioners (preferring the term "information security" or "infosec"), even while its cachet has grown for policymakers.[82]

The UK again offers an apt case study: its successful export of a "National Cybersecurity Centre" model is strategically valuable, enabling its partners to be better protected and share information with the UK, but also symbolically valuable, communicating an appearance of cross-government coordination and public-private alignment that benefits it domestically and abroad.[83]

3. Multilateral and national approaches to strategic digital technologies

This section moves from the analysis of strategic value categorized by technology to examine national and international approaches to these technologies. This involves a two-tiered examination: at the international level, through countries' contributions to multilateral initiatives, and at the national level through individual country strategies. Our review concentrates on the thirteen countries that have made individual contributions to the UN Global Digital Compact (GDC), alongside an additional analysis of the contributions from the European Union.

The GDC has a broad understanding of multilateralism, and convenes representatives of civil society, academia, technical communities, and the private sector alongside those of government. Submissions to the GDC reflect this by targeting a broad audience beyond just state entities. The documents from the GDC and national technology strategies together outline how states prioritize their technology policies.

> *The abstract and uniform language in GDC statements hides differences in how countries view the strategic importance of certain digital technologies, making it hard to identify clear distinctions between them.*

The GDC emphasizes inclusivity and a holistic view of technology, setting a benchmark for engagement. Meanwhile, national strategies outline each state's initial stance, policy priorities and long-term ambitions more clearly than the broader discussions at the GDC.

While alternative multilateral forums, such as the Global Partnership on AI, which focuses on ethical AI development, or the ITU World Radiocommunication Conference, which delves into spectrum management critical for 5G/6G technologies, could have served as platforms for this two-tiered examination, the GDC was selected for its broader scope. The GDC uniquely encompasses a wide range of digital technologies within a single framework, aligning with the report's objective to adopt an inclusive approach that captures the full spectrum of digital technology issues, rather than focusing on niche or specific technological domains.

The analysis shows that the abstract and uniform language in GDC statements hides differences in how countries view the strategic importance of certain digital technologies, making it hard to identify clear distinctions between them. Yet, for national strategies, the analysis is particularly helpful in showing how countries perceive the value of certain digital technologies.

3.1 Strategic digital technologies at the GDC

Proposed by the UN Secretary-General as a contribution to the UN Summit of the Future planned for September 2024, the GDC is a central element of the efforts to reform the UN's multilateral system. As the official technology track for these discussions,[84] this makes the GDC a test case at the global level.

The first step in this analysis was to identify all states to have submitted individual contributions to GDC consultations: Austria, China, Cuba, El Salvador, France, Iran, Japan, the Netherlands, Poland, Singapore, Switzerland, the United Kingdom, and the United States. Between June 2022 and April 2023, over 160 governments contributed to online consultations – the vast majority as part of regional groupings. By comparison, only the 13 governments above submitted an individual contribution. The government of Germany, for example, which together with Mexico, India, and Kenya as local partners facilitated regional consultations with multistakeholder participants in the Americas, Asia and Africa, did not submit a national contribution separate from the contribution filed by the European Union. Also, none of the other regional facilitator countries opted to provide individual inputs. Non-state actors filed more than 90% of the 178 individual submissions received by April 2023.

Individual state submissions are therefore a relatively small part of the overall GDC consultation process. However, given the difficulties in untangling individual state positions from regional groupings, and the importance of individual state policy for the framework of strategic value above – including the element of nationalizations – the individual submissions are most relevant for this report. Helpfully, despite its narrowness in relation to

the consultation process overall, this selection process captures a range of state positions, including EU member states, participants of minilateral arrangements such as the Quad, as well as smaller trade- and technology-driven economies, and countries that are subject to technology export restrictions. We make one exception to this rule by including the EU submission as part of the analysis below; we justify this exception not because one can ascertain individual state positions through this regional submission, but because the EU is a crucial independent actor.

These contributions show convergence on the broad benefits digital technology can provide as an enabler of economic and social activity [85] by connecting markets and people. Ambitions to spur progress towards the sustainable development goals (SDGs) notably drive discussions about digital innovations at the UN level.

This general agreement notwithstanding, the contributions emphasize that such progress is not a given or inherent to technology, but conditional on appropriate safeguards that guide its application.

For some states, the GDC offers a platform for communicating structural imbalances or restrictions that are being perceived as unfair or disproportionate in their targeting. For example, Iran sought to link its efforts to overturn international sanctions affecting its economy to the ability to make progress towards the SDGs. In its submission, Iran called for the dismantling of restrictive measures that limit countries in their access to emerging communication and information technologies that underwrite national digital development.[86]

Similarly, Cuba's submission points to such external influences on the resources of countries that constrain possibilities for indigenous technology development in the long-term.[87] Cuba explicitly cites financial and trade restrictions levied by the United States as exacting a high toll on its ICT sector. In contrast, Cuba claims that new approaches to automation may, for example, develop economic production capacities that afford advantages to less technologically advanced countries by allowing for import substitution.[88] Calls as these by Cuba and Iran show that priorities may be linked to overlapping factors of strategic value, as in this case externalities of trade restrictions and the access to and control over the technology supply chain.

Mobilization against adverse conditions may also appeal to the interoperability factor. Efforts by the UK[89] and the Netherlands[90] seek to raise awareness about non-technical barriers to connectivity, such as content blocks or Internet shutdowns. Framing connectivity in terms of interoperability at the content layer, these statements turn to the GDC as a platform to address internet fragmentation concerns beyond the logic level of protocols and technical specifications that are the focus of international standard development organisations. In contrast, other states seek to use the GDC to communicate messages around the value of broader participation. For example, GDC submissions from European countries especially identified support for engagement in digital technology development as priority areas.

However, beyond well-trodden arguments around structural inequalities in the international system, GDC submissions shed little light on states' position regarding strategic digital technology, especially the six factors detailed in Section 1.

The EU submission to the GDC is a notable exception in this regard among the contributions of individual countries. The submission contextualizes its positions through consistent references to relevant EU action plans, policy programmes, previous communications, as well as pieces of legislation for each technology area addressed in its statement to demonstrate its engagement on the issue.[91]

These interlinkages between the EU's GDC statement and its domestic policy agenda allow for a straightforward mapping of the strategic value identified in the referenced EU documents to the corresponding GDC positions.

Addressing the role of network effects, the submission connects the EU's initiatives in developing a legal framework to manage risks related to AI systems – most principally, the AI Act – to its efforts at building trusts through rules that apply equally within the European Union. The contribution to the GDC argues that trust in the protection of health, safety and fundamental rights increases as the same requirements for developing, deploying and using the technology are introduced across all member states.

In addition, the contribution discusses the network effects of the EU's single market, invoking obligations under the EU's Digital Services Act. This legislation mandates that major online platforms grants access to their data and algorithmic systems to member states and research as a condition for market access.[92]

As a consensus-driven actor, the EU in its multilateral engagement is more closely bound to pre-agreed baselines. Its GDC submission appears to reflect this through its emphasis on presenting and explaining the EU's domestic agenda and opportunities to interface internationally. As a result of this integration of domestic achievements into multilateral messaging, these positions, however, also transparently and consistently communicate priorities, adding to their credibility and supporting the identification of areas for reliable cooperation.

As a consensus-driven actor, the EU in its multilateral engagement is more closely bound to pre-agreed baselines. Its GDC submission appears to reflect this through its emphasis on explaining the EU's domestic agenda and opportunities to interface internationally.

3.2 National digital technology strategies

The next step in our analysis is to explore relevant national strategies for select states submitting individual contributions to the GDC. Again, these states were selected to encompass a range of diplomatic and political positions, as well as technological perspectives and priorities.

Most of these states had published at least one strategy, with scope ranging from "technology" in general, to the increasingly common designation "critical and emerging technologies (CET)". We can see the term "CET" as another way of describing strategic value: because either a technology is rapidly changing the international landscape (it is emerging), or it underpins key facets of a nation or society (it is critical). A list of the strategies included is in Table 3 below, although some states had published multiple sub-strategies. For example, the UK's Quantum or Semiconductor Strategies fall under its International Technology Strategy, while the US's CET strategy included a separate standards strategy in 2023.

With the exception of the European Economic Security Strategy as a supranational document, this selection only considered national strategy documents published until April 2023 to align with the timeline of assessed GDC submissions. The selection of national strategies was based on documents that address technology as comprehensively as the GDC, covering a six-year span. Of course, the rapid evolution of digital technologies means that much has changed in these six years, with the time difference itself partly contributing to differences in content.

> *"We can see the term "critical emerging technologies (CET)" as another way of describing strategic value: because either a technology is rapidly changing the international landscape (it is emerging), or it underpins key facets of a nation or society (it is critical)."*

While these strategies do not focus on specific technologies, the remainder of this section highlights elements of these strategies that align with different elements of the framework of strategic value put forward in Section 1. The purpose of this analysis is to show the interpretative, rather than the explanatory value of this framework: in other words, to demonstrate how it provides a cogent differentiation between different factors in strategic value, rather than contributing to state decisions around strategic value. Explanatory analysis would require a more extensive, rigorous analysis beyond the scope of this report.

Table 3: Digital technology strategies

State	Strategy Document	Year
Australia	International Cyber and Critical Technology Engagement Strategy	2021
Austria	Digital Action Plan	2020
China	Jointly Build a Community with a Shared Future in Cyberspace	2022
Cuba	Comprehensive Policy for the Improvement of the Computerization of the Society in Cuba	2017
Denmark	Strategy for Tech Diplomacy	2021
El Salvador	Law to Promote Innovation and Manufacturing of Technologies	2023
EU	European Economic Security Strategy	2024
France	International Digital Strategy	2017
Iran	Science, Technology and Innovation in Iran	2023
Japan	Basic Guideline for Critical Technologies	2022
Netherlands	International Cyber Strategy	2023
Poland	Cybersecurity Strategy	2019
Singapore	Smart Nation: The Way Forward	2018
Switzerland	Digital Foreign Policy Strategy	2020
UK	International Technology Strategy	2023
US	National Strategy for Critical and Emerging Technologies	2020

i) Importance

In these strategies, states express the importance of digital technologies in several ways. France points to developing the EU's digital internal market as the first objective, which in this vision can then act as an incubator for European technological leadership on industry 4.0, artificial intelligence, and blockchain technologies.[93] The UK's International Technology Strategy links the safe use and development of technologies to the goals of protecting fundamental rights, fostering innovation, enabling sustainable growth, and ensuring fair competition.[94]

More specifically, the UK National Semiconductor Strategy – one of the sub-strategies within the International Technology Strategy listed above - characterizes this sector as "essential to unlock future innovation in the broad range of technologies which they enable".[95] The document refers to semiconductors as underwriting the UK's status as "science and technology superpower". It further assesses semiconductors as directly contributing to the objectives outlined in its strategies for quantum computing, cybersecurity, AI, and space, alongside broader societal goals, such as achieving net-zero carbon emissions by 2050.

In contrast, for states with self-imposed restrictions – such as bans or censorship against certain platforms – or external measures – including sanctions or export controls – digital technologies present different opportunities and challenges. Propped up by immense state subsidies, these conditions have been likened to a 'gilded cage' for Chinese fledgling industries,[96] which have lifted up technology companies, such as Baidu, Alibaba, Tencent and Huawei, to become national champions.[97] Like France, China also highlights regional as well as national importance, through its assistance in the rollout of mobile networks, provision of cloud services, and the laying of subsea cables for countries participating in the Digital Silk Road component of the Belt and Road Initiative.[98]

ii) Externalities

The clearest externalities for these states are connected to cybersecurity, as the most well-established national security priority. Recognizing cyber-enabled economic espionage as a national security threat, the United States in consultation with international partners has sought to hold perpetrators accountable through indictments and sanctions for close to a decade.[99] Cyber espionage also gives rise to concerns about transnational digital repression. A growing market segment "selling digital insecurity"[100] enables actors seeking to control populations that otherwise might lack the necessary technical capabilities.[101] Consequently, as part of its International Cyber Strategy, the Netherlands points to the need to offset risks of abuse by establishing a clear regulatory basis, for instance to prescribe how to use big data analysis to stop crime.[102]

The externalities of AI also feature heavily for these states. Expressing concerns about the effects of AI on the offensive-defence balance, states emphasize the importance of responsible experimentation to ensure net benefits for defenders. Outside the scope of strategies reviewed in full for this section but indicative of these same concerns, the Euro-

pean External Action Service addresses the influence of generative AI on this competition and the stakes involved in protecting the integrity of the European Parliamentary elections across 27 countries and a community of 24 languages from foreign information manipulation and interference threats.[103]

Concentrating on effectiveness, Australia's International Cyber and Critical Technology Engagement Strategy explores the potential inherent in AI as a tool for streamlining compliance and regulatory oversight (RegTech).[104] Similarly, Singapore has sought to harness AI-enabled analytics to design inclusive political processes and strengthen social cohesion.[105]

iii) Nationalization

Most states grappled with the perceived necessity of nationalization for strategic digital technologies, demonstrating awareness of its downsides. The UK Technology Strategy acknowledges the risk of spurring "technological protectionism". To this end, the document emphasizes agility as a design principle for export control regimes, noting the challenge of keeping pace with the rapid development of dual-use technologies.[106]

Efforts to keep the scope of nationalization narrow are also mirrored in the US National Strategy for CETs. References to export control frameworks put the focus on developing targeted measures that govern the appropriate aspects of critical technology.[107] The Biden administration described this as "small yard, high fence" approach,[108] which aims to ensure robust protections for limited carefully identified technology areas. For Huawei specifically, commentators have argued that export restrictions may also impose costs on own or allied companies at least in the short to medium term, as high-volume contracts are forfeited[109] or can only be maintained after the completion of lengthy licensing applications conducted at considerable political risk.[110]

In line with declarations by the UK, provisions in the US strategy urge protections against illicit efforts by competitors to acquire intellectual property, acknowledging that export controls may need to account for concerted attempts to circumvent such restrictions.[111] In the same vein, the EU's Economic Security Strategy calls for the integration of technology security and technology leakage into risk assessments.[112] To this end, the strategy tasked the European Commission with the identification of technology areas that are critical to economic security. Out of the ten technology areas specified in October 2023, the Commission identified four technology areas as presented with the most sensitive and urgent risks. For these four clusters, which include advanced semiconductor technologies, AI technologies, quantum technologies, and biotechnologies, the Commission proposed that member states conduct a joint risk assessment in collaboration with the Commission.

In an apparent reaction to like-minded coalitions among democratic partner countries, China notes its opposition to "narrow-minded factionalism"[113] in combination with the need to promote open cooperation. China phrases this as win-win cooperation with mu-

tual benefits for partners, and explicitly contrasts this with approaches described as designed for "decoupling and severing supply chains" that would result in mutual losses for both the countries pursuing and targeted by such strategies.[114]

iv) Interoperability and standards

Concerns around the strategic impact of standardization processes - including data protection regulation - are present throughout the reviewed strategy documents. The US even published a separate National Standards Strategy for Critical and Emerging Technology, adopted by the US government in May 2023.[115] The strategy seeks to address what it identifies as undue influence of standard development processes.

The document calls out attempts by China to secure support for its standard proposals through investment pledges and economic coercion. Similarly, the Quad working group on critical and emerging technologies has acted as a platform for Australia and the United States, along with India and Japan, to define principles for technology standards development in cooperation with other like-minded states.[116] Frameworks for coordination have drawn interest from smaller technologically advanced, trade-oriented economies, such as Singapore, as an opportunity to bring greater visibility to their positions.

The EU Economic Security Strategy approaches standardization as an element of 'soft power'.[117] Shaping the implementation of technology, standards in this perspective provide a technical way to reducing the possibilities of technology abuse.

To prevent technology leakage, the EU also highlights the need to protect the underlying intellectual properties of standards.[118]

More generally, calls by states for protected free data flow recognize cross-border data transfers as precondition for participation in foreign markets. As more states adopt data protection regimes, data adequacy frameworks have received increasing attention to ensure continued market access in light of the implementation of robust data protections[119].

v) Network effects

Network effects were generally not discussed in the strategies analysed. In an exception to this rule, diplomatic initiatives of the Netherlands identify network effects as a means for mainstreaming best practices to eliminate the influence of biases in the design, development, and deployment of AI-enabled solutions that have been developed domestically to extend their protections.[120]

The EU also invokes landmark legislation, including the NIS2 Directive, Cyber Resilience Act and Cyber Solidarity Act, for its capacity to set baseline resilience measures and supply chain protections and to harmonize reporting requirements and testing procedures.[121]

The main relevance of network effects for these states seems not to be the network effects of the technologies themselves, but network effects of certain policy approaches. Building coalitions to promote uptake, the UK National Cyber Security Centre and the US Cybersecurity and Infrastructure Security Agency[122] as well as the Australian Cyber Security Centre[123] have collaborated with international partners in the design of appropriate safeguards to guide the safe and secure development and deployment of AI. Similarly, to navigate sensitive security concerns with potential foreign policy ramifications, EU member states jointly developed a toolbox comprising risk mitigating measures to ensure the cybersecurity of 5G networks, to provide a coordinated approach[124].

The European Commission traces the rationale for the Economic Security Strategy to similar considerations. In the absence of a coordinated approach, the strategy contends partners will be left to develop alliances on their own, with the risk of dispersing resources to reduced effect, potentially allowing less well-intentioned actors to seize on and exploit differences[125].

vi) Capability and control

A variety of states discussed issues around the independence of access to and control of digital technologies in their strategic documents, especially in relation to "big tech". Denmark described "data monopolies" controlled by global technology companies as a barrier to entry that limit smaller technology companies in the ability to participate in innovation in data-driven business models.[126] Highlighting the need to support the development of a domestic technology and industrial base, Denmark pushes for high-revenue technology companies to pay commensurate taxes. While Denmark focuses on a taxation-based approach, the UK adopts a more flexible risk framing.

The UK's International Technology Strategy references an overhauled telecoms security framework implemented under the Telecommunications (Security) Act 2021, which is supported by new government authorities to regulate which goods and services public ISPs source from high-risk vendors.[127]

Concerns about big tech also appear in very different states. Responding to perceived attempts of weaponized interdependence, the proposal to "Jointly Build a Community with a Shared Future in Cyberspace", issued by China's State Council, challenges initiatives designed to exploit "one's own strengths to undermine the security of other countries' supply chains".[128] The white paper labels leveraging other states' technological dependence to control access to technologies as "abusing state power and violating market principles and trading rules". There is no consideration of the possible applications of this argument to China's technological dominance itself. In a positive expression of the same sentiment, the Department of Science and Technology within the Iranian President's Office framed renewed economic restrictions following the US withdrawal from the Joint Comprehensive Plan of Action 2018 as an opportunity for Iranian businesses to take advantage of the lack of foreign competitors and "clone and localize the international

platforms and services".[129] Conversely, the EU Economic Security Strategy refers to well-justified exclusions of organizations from digital capacity projects as part of protecting the European Union's autonomy, if they are controlled by countries deemed to pose proliferation or other security concerns.[130] To reduce and prevent strategic dependencies across the EU, the strategy foresees the creation of a Strategic Technologies for Europe Platform (STEP).[131] The platform, on which the Council and the European Parliament reached a provisional agreement in February 2024, provides investment in digital technology, among other areas, with the goal to strengthen development and manufacturing capacities in support of the EU's sovereignty and competitiveness.[132]

Notably, the EU's Economic Security Strategy also addresses the need to protect member states from external efforts that aim to use capability or control for coercion.[133] To deter trade or investment restrictions designed to force a change in policy, the EU has set up an Anti-coercion Instrument, which provides for mechanisms to adopt countermeasures.[134]

Conclusion and future research

The purpose of this report was to examine the nature of strategic digital technologies and their role in international affairs. Our investigation is grounded in three principal contributions: Firstly, we introduced a novel conceptual framework that expands upon existing theories to better assess the strategic dimensions of digital technologies. This framework is a significant advancement, offering a more detailed understanding of how these technologies hold varying degrees of strategic value across different indicators and contexts.

Secondly, the report provides an examination of key strategic digital technologies: AI, cybersecurity, quantum technologies, 5G, the internet of things and cloud computing. This analysis is essential for comprehending the multifaceted strategic properties and implications of these technologies.

Thirdly, the analysis of national and international approaches to these technologies, particularly through the lens of the UN Global Digital Compact (GDC) and individual state strategies, shows the wide range of perceived economic and societal impacts of digital technologies. This overview shows indications that the strategic value framework proposed can highlight alignments in state perspectives that form the basis of political declarations of shared values and goals. By undercovering these alignments, this analysis can help identify promising projects for future international cooperation.

Looking ahead, there is a clear need for further research, especially in conducting detailed case studies on the application of these technologies across different national settings. Such research will not only deepen our understanding of the strategic roles of digital technologies but also facilitate more effective multilateral collaborations.

Endnotes

[1] Parts 1, 2 and 3 of this Deliverable 5.1 are based on a working paper by Shires and Smeets. Part 3 is also based on a forthcoming book chapter by Bund.

[2] David A. Baldwin, *Economic Statecraft* (Princeton, New Jersey: Princeton University Press, 1985).

[3] Jeffrey Ding and Allan Dafoe. "*The Logic of Strategic Assets: From Oil to AI.*" Security Studies 30, no. 2 (2021): 182–212. https://doi.org/10.1080/09636412.2021.1915583.

[4] See e.g. Herrera, Geoffrey L. Technology and International Transformation: *The Railroad, the Atom Bomb, and the Politics of Technological Change.* Albany, NY: State University of New York Press, 2007.

[5] Ding and Dafoe. 207

[6] Ding and Dafoe. 210

[7] We define digital technologies as those that rely on digital or binary (0 and 1) signals, primarily coded into and transmitted via computer systems and networks. We recognize that quantum computers using qubits (bits that permit computation in additional states to 0 and 1) are not binary (indeed, that is their main advantage), but they are similarly integrated into computer systems and networks, and so we include them in this report.

[8] Ibid.

[9] Jack Goldsmith and Tim Wu, Who Controls the Internet?: Illusions of a Borderless World (New York, NY: Oxford University Press, 2006).

[10] "The Evolution of Wi-Fi Technology and Standards," IEEE Standards Association, published May 16, 2023, https://web.archive.org/web/20240204203131/https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/#:~:text=IEEE%20802.11%E2%84%A2%20is%20the,for%20Wi%2DFi%20wireless%20networks.&text=Wi%2DFi%20TECHNOLOGY-,Wi%2DFi%20technology%20is%20based%20on%20the%20IEEE%20802.11%E2%84%A2,we%20communicate%20and%20access%20information.

[11] "Web Standards," World Wide Web Consortium (W3C), accessed February 14, 2024, https://web.archive.org/web/20240214164817/https://www.w3.org/standards/.

[12] Tim Rühlig, "The Shape of Things to Come: The Race to Control Technical Standardisation," European Union Chamber of Commerce in China, 2021, https://web.archive.org/web/20231203045951/https://eboworldwide.eu/wp-content/uploads/2023/06/The_Shape_of_Things_to_Come_English_Final966.pdf, 54.

[13] Lifshitz-Assaf, Hila, and Frank Nagle. "The Digital Economy Runs on Open Source. Here's How to Protect It." Harvard Business Review, September 2, 2021. https://hbr.org/2021/09/the-digital-economy-runs-on-open-source-heres-how-to-protect-it. Of course, open-source communities are vulnerable to corporate influence and other forms of exclusion in other ways.

[14] Geoffrey Parker, Marshall van Alstyne, and Sangeet Paul Choudary, Platform Revolution: How Networked Markets Are Transforming the Economy - and How to Make Them Work for You (New York, London: W. W. Norton & Company, 2016).

[15] Christopher J. Tozzi, For Fun and Profit: A History of the Free and Open Source Software Revolution, History of Computing (Cambridge, MA: MIT Press, 2017).

[16] Donald Deibert et al., Access Denied: The Practice and Policy of Global Internet Filtering, Information Revolution and Global Politics (Cambridge: The MIT Press, 2008). https://doi.org/10.7551/mitpress/7617.001.0001.

[17] Also see new research project of Rebecca Slayton. "Profile of Rebecca Slayton," Department of Science and Technology Studies, Cornell University, accessed February 14, 2024, https://web.archive.org/web/2/https://sts.cornell.edu/rebecca-slayton.

[18] Daniel W. Drezner, Henry Farrell, and Abraham L. Newman, The Uses and Abuses of Weaponized Interdependence (Washington, DC: Brookings Institution Press, 2021).

[19] O.L. van Daalen, "The right to encryption: Privacy as preventing unlawful access," Computer Law & Security Review 49 (2023), https://doi.org/10.1016/j.clsr.2023.105804.

[20] Nicholas Davis, Mark Esposito, and Landry Signé, "The anatomy of technology regulation," Brookings Institution, February 17, 2022, https://web.archive.org/web/2/https://www.brookings.edu/articles/the-anatomy-of-technology-regulation/.

[21] Alexander Lanoszka, Military Alliances in the Twenty-First Century (Cambridge, UK, Medford, MA: Polity Press, 2022).

[22] Janka Oertel, "Why the German Debate on 5G and Huawei is Critical," German Marshall Fund, accessed February 14, 2024, https://web.archive.org/web/2/https://www.gmfus.org/news/why-german-debate-5g-and-huawei-critical.

[23] Jacquelyn Schneider, "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War," Journal of Strategic Studies 42, no. 6 (2019), doi:10.1080/01402390.2019.1627209.

[24] Ibid.

[25] Max Smeets, No Shortcuts: Why States Struggle to Develop a Military Cyber-Force (London: C. Hurst & Co Publishers Ltd, 2022).

[26] Robert Chesney, James Shires and Max Smeets, eds., Cyberspace and Instability (Edinburgh: Edinburgh University Press, 2023), [20] Nicholas Davis, Mark Esposito, and Landry Signé, "The anatomy of technology regulation," Brookings Institution, February 17, 2022, https://web.archive.org/web/2/https://www.brookings.edu/articles/the-anatomy-of-technology-regulation/.

[27] Brendon J. Cannon and Ash Rossiter, "Unraveling Japan's Aircraft Carrier Puzzle: Leveraging Carriers' Symbolic Value," *Asian Security* 18, no. 1 (2022), doi:10.1080/14799855.2021.1982897.

[28] Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies,* Reprinted with corrections (Oxford: Oxford University Press, 2017).

[29] Ben Buchanan und Andrew Imbrie, *The new fire: War, peace, and democracy in the age of AI* (Cambridge: The MIT Press, 2022).

[30] Chesney, Shires and Smeets, Cyberspace and Instability.

[31] Marion Messner, James Shires, and Armida van Rij, "Quantum technology competition must not become an arms race", *The World Today,* Chatham House, 29 September 2023, https://www.chathamhouse.org/publications/the-world-today/2023-10/quantum-technology-competition-must-not-become-arms-race.

[32] Michal Krelina, „Quantum technology for military applications." *EPJ Quantum Technology* 8, Nr. 1 (2021), doi:10.1140/epjqt/s40507-021-00113-y.

[33] Charles Q. Choi, "The Race to Build a Fault-Tolerant Superconducting Quantum Computer," IEEEE Spectrum, February 2, 2022, https://web.archive.org/web/2/https://spectrum.ieee.org/fault-tolerant-quantum-computing.

[34] On security implications from a European perspective see: Jan-Peter Kleinhans, "5G vs. National Security: A European Perspective," Stiftung Neue Verantwortung, February 2019, https://web.archive.org/web/20230925104112/https://www.stiftung-nv.de/de/publikation/5g-vs-national-security.

[35] Khaled B. Letaief, Wei Chen, Yuanming Shi, Jun Zhang, and Ying-Jun Angela, "The Roadmap to 6G: AI empowered wireless networks," IEEE Communications Magazine, 57, 8, 2019, https://doi.org/10.1109%2Fmcom.2019.1900271.

[36] Paul Triolo, Kevin Allison, Clarise Brown, "The Geopolitics of 5G," Eurasia Group, November 2018, https://web.archive.org/web/2/https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf; see also Roxana Radu, Cedric Amon, The governance of 5G infrastructure: between path dependency and risk-based approaches, Journal of Cybersecurity, Volume 7, Issue 1, 2021, https://doi.org/10.1093/cybsec/tyab017.

[37] Derek S. Reveron and John E. Savage, Security in the cyber age: An introduction to policy and technology (Cambridge, United Kingdom: Cambridge University Press, 2023).

[38] James Manyika and Michael Spence, "The Coming AI Economic Revolution: Can Artificial Intelligence Reverse the Productivity Slowdown?," Foreign Affairs Magazine, October 24, 2023, accessed February 29, 2024, https://www.foreignaffairs.com/world/coming-ai-economic-revolution.

[39] Forrest E. Morgan et al., Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World, with the assistance of Forrest E. Morgan et al. (RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RR3139-1.html; Sarah Grand-Clément, "Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain," 2023, https://unidir.org/publication/artificial-intelligence-beyond-weapons-application-and-impact-of-ai-in-the-military-domain/; ICRC, "What You Need to Know About Artificial Intelligence in Armed Conflict," October 6, 2023, accessed February 29, 2024, https://www.icrc.org/en/document/what-you-need-know-about-artificial-intelligence-armed-conflict.

[40] James Johnson, "Automating the OODA Loop in the Age of Intelligent Machines: Reaffirming the Role of Humans in Command-and-Control Decision-Making in the Digital Age," Defence Studies 23, no. 1 (2023), https://doi.org/10.1080/14702436.2022.2102486.

[41] Paul Scharre, Four Battlegrounds: Power in the Age of Artificial Intelligence, Paperback edition (New York, NY: W.W. Norton & Company, 2023); Pablo Chavez, „Vassals vs. Rivals: The Geopolitical Future of AI Competition," Lawfare, August 3, 2023, https://www.lawfaremedia.org/article/vassals-vs.-rivals-the-geopolitical-future-of-ai-competition.

[42] Derek S. Reveron and John E. Savage, Security in the Cyber Age: An Introduction to Policy and Technology (Cambridge, United Kingdom: Cambridge University Press, 2024), https://doi.org/10.1017/9781009308564.

[43] Keiko Kono and Samuele De Tomas Colatin, "National approaches to the supply chain cybersecurity: Taking a more restrictive stance against high-risk vendors," Cooperative Cyber Defence Centre of Excellence, 2023, https://www.ccdcoe.org/uploads/2023/05/Supply_Chain_Cybersecurity.pdf.

[44] Derek S. Reveron and John E. Savage, "Cybersecurity Convergence: Digital Human and National Security," Orbis 64, no. 4 (2020), https://doi.org/10.1016/j.orbis.2020.08.005.

[45] James Andrew Lewis and Georgia Wood, Quantum Technology: Applications and Implications (2023), https://www.csis.org/analysis/quantum-technology-applications-and-implications.

[46] Edward Parker, Daniel Gonzales and Ajay K. Kochhar, An Assessment of the U.S. And Chinese Industrial Bases in Quantum Technology, Research reports RR-A869-1 (Santa Monica, Calif.: RAND Corporation, 2022). https://doi.org/10.7249/RRA869-1 ; Edward Parker, ASSESSMENT of U.S.-ALLIED NATIONS' INDUSTRIAL BASES in QUANTUM TECHNOLOGY (Santa Monica, Calif.: RAND Corporation, 2023), https://doi.org/10.7249/RRA2055-1.

[47] Georg E. Riekeles, "Quantum technologies and value chains: Why and how Europe must act now," European Policy Centre, March 2023, https://www.epc.eu/content/PDF/2023/Quantum_Technologies_DP.pdf; Sujai Shivakumar, Charles Wessner and Thomas Howell, Quantum Can't Be Business as Usual: Issues for the Reauthorization of the National Quantum Initiative Act (2023), https://www.csis.org/analysis/quantum-cant-be-business-usual-issues-reauthorization-national-quantum-initiative-act; Elsa B. Kania and John Costello, "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership," Center for New American Security, September 2018, https://www.cnas.org/publications/reports/quantum-hegemony.

[48] Oxford Economics, "The Global Economic Potential of 5G-enabled Technology," March 2023 https://www.oxfordeconomics.com/wp-content/uploads/2023/03/GlobalEconomicPotential5G_290323.pdf.

[49] World Economic Forum, "The Impact of 5G: Creating New Value across Industries and Society," 2020, https://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf.

[50] Antonio Calcara, "From Quiet to Noisy Politics: Varieties of European Reactions to 5G and Huawei," Governance 36, no. 2 (2023), https://doi.org/10.1111/gove.12674.

[51] IOT Analytics, "State of IoT 2023," May 2023, https://iot-analytics.com/number-connected-iot-devices/.

[52] Christos Stergiou et al., "Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT," Sustainable Computing: Informatics and Systems 19 (2018), https://doi.org/10.1016/j.suscom.2018.06.003 ; Carsten Maple, "Security and Privacy in the Internet of Things," Journal of Cyber Policy 2, no. 2 (2017), https://doi.org/10.1080/23738871.2017.1366536.

[53] Nathaniel Kim, Trey Herr, and Bruce Schneier, "The Reverse Cascade: Enforcing Security on the Global IoT Supply Chain," Atlantic Council, June 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/06/Reverse-Cascade-Report-v3.1.pdf.

[54] Tianjiu Zuo, Justin Sherman, Maia Hamin, and Stewart Scott, "Critical Infrastructure and the Cloud: Policy for Emerging Risk," Atlantic Council, July 2023, https://dfrlab.org/wp-content/uploads/sites/3/2023/07/critical_infra_and_the_cloud.pdf.

[55] IBM Cloud Team, "Top 7 Most Common Uses of Cloud Computing," August 1, 2022, https://www.ibm.com/blog/top-7-most-common-uses-of-cloud-computing/; Sandipan Sarkar, Soma Mukherjee, and Diptanu Roy, "Living in a data sovereign world," IBM, October 16, 2023, https://www.ibm.com/blog/living-in-a-data-sovereign-world/.

[56] Trey Herr, "Four Myths About the Cloud: The Geopolitics of Cloud Computing," Atlantic Council, August 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/four-myths-about-the-cloud-the-geopolitics-of-cloud-computing/.

[57] Jari Haiston, "IoT Protocols vs IoT Standards," Symmetry Electronics, July 17, 2023, https://web.archive.org/web/2/https://www.symmetryelectronics.com/blog/iot-protocols-vs-iot-standards/#:~:text=An%20IoT%20(Internet%20of%20Things,security%20in%20an%20IoT%20environment.

[58] Daphne Leprince-Ringuet, "Quantum computing is at an early stage. But investors are already getting excited," ZDNET, September 15, 2021, https://web.archive.org/web/20230720223123/https://www.zdnet.com/article/quantum-computing-is-at-an-early-stage-but-investors-are-already-getting-excited/.

[59] Mina Narayanan, Alexandra Seymour, Heather Frase, and Karson Elmgren, "Repurposing the Wheel: Lessons for AI Standards" (Center for Security and Emerging Technology, November 2023). https://doi.org/10.51593/20230021; Arthur Holland Michel, "Recalibrating Assumptions on AI". (Chatham House, April 2023), DOI: 10.55317/9781784135621.

[60] Kieron O'Hara und Wendy Hall, Four internets: Data, geopolitics and governance of cyberspace (New York, NY: Oxford University Press, 2021).

[61] Petroc Taylor, "5G Patents held by leading companies worldwide as of September 2021," Statista, November 2023, https://web.archive.org/web/2/https://www.statista.com/statistics/1276457/leading-owners-of-5g-patents-worldwide/.

[62] "Leveraging American Communications Leadership with Open Radio Access Networks," Hearing before the US House of Representative Subcommittee on Communications and Technology, January 17, 2024, https://web.archive.org/web/2/https://energycommerce.house.gov/events/communications-and-technology-subcommittee-hearing-leveraging-american-communications-leadership-with-open-radio-access-networks.

[63] Open RAN Policy Coalition, "Open RAN Security in 5G," April 2021, https://web.archive.org/web/2/https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf.

[64] Mina Narayanan, Alexandra Seymour, Heather Frase, and Karson Elmgren, "Repurposing the Wheel: Lessons for AI Standards" (Center for Security and Emerging Technology, November 2023). https://doi.org/10.51593/20230021.

[65] Robert W. Gregory et al., "The Role of Artificial Intelligence and Data Network Effects for Creating User Value," Academy of Management Review 46, no. 3 (2021), https://doi.org/10.5465/amr.2019.0178.

[66] William Alan Reinsch et al., Optimizing Export Controls for Critical and Emerging Technologies (2023), https://www.csis.org/analysis/optimizing-export-controls-critical-and-emerging-technologies; Tim Hwang and Emily S. Weinstein, "Decoupling in Strategic Technologies From Satellites to Artificial Intelligence," Center for Security and Emerging Technology, July 2022, https://cset.georgetown.edu/publication/decoupling-in-strategic-technologies/.

[67] Alexis Hancock, "We Encrypted the Web," Electronic Frontier Foundation, December 27, 2021, https://www.eff.org/deeplinks/2021/12/we-encrypted-web-2021-year-review.

[68] Arun Vishwanathan, The Weakest Link: How to Diagnose, Detect, and Defend Users from Phishing (Cambridge, Massachusetts: The MIT Press, 2022).

[69] Naurin F. Khan, Naveed Ikram, and Sumera Saleem, "Effects of Socioeconomic and Digital Inequalities on Cybersecurity in a Developing Country," Security Journal, 2023, https://doi.org/10.1057/s41284-023-00375-4.

[70] Oskar van Deventer et al., "Towards European Standards for Quantum Technologies," EPJ Quantum Technology 9, no. 1 (2022), https://doi.org/10.1140/epjqt/s40507-022-00150-1.

[71] William Alan Reinsch et al., 2023; Sam Howell, To Restrict, or Not to Restrict, That Is the Quantum Question, Lawfare, May 2023, https://www.lawfaremedia.org/article/to-restrict-or-not-to-restrict-that-is-the-quantum-question.

[72] Niels ten Oever and Stefania Milan, "The Making of International Communication Standards: Towards a Theory of Power in Standardization," Journal of Standardisation, 2022, https://doi.org/10.18757/JOS.2022.6205.

[73] Dan Littmann et al., "5G: The chance to lead for a decade," Deloitte, 2018, https://www2.delDoitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf.

[74] Elsa B. Kania,"Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy," Center for New American Security, November 2019, https://www.cnas.org/publications/reports/securing-our-5g-future; James Sullivan and Rebecca Lucas, "5G Cyber Security A Risk-Management Approach," Royal United Services Institute, February 2020, https://static.rusi.org/20200602_5g_cyber_security_final_web_copy.pdf; Jan-Peter Kleinhans, "Whom to trust in a 5G world? Policy recommendations for Europe's 5G challenge," Stiftung Neue Verantwortung, December 2019, https://www.stiftung-nv.de/sites/default/files/whom_to_trust_in_a_5g_world.pdf.

[75] Keith Dickerson et al., "Standards for the IoT," in IoT Platforms, Use Cases, Privacy, and Business Models: With Hands-on Examples Based on the VICINITY Platform, 1st edition 2021 (Cham: Springer International Publishing, 2021), https://doi.org/10.1007/978-3-030-45316-9_6.

[76] Sang-Jin Ahn, "Three Characteristics of Technology Competition by IoT-Driven Digitization," Technological Forecasting and Social Change 157 (2020), https://doi.org/10.1016/j.techfore.2020.120062 ; Harald Edquist, Peter Goodridge, and Jonathan Haskel, "The Internet of Things and Economic Growth in a Panel of Countries," Economics of Innovation and New Technology 30, no. 3 (2021), https://doi.org/10.1080/10438599.2019.1695941.

[77] André Cirne et al., "IoT Security Certifications: Challenges and Potential Approaches," Computers & Security 116 (2022), https://doi.org/10.1016/j.cose.2022.102669.

[78] Ilsa Godlovitch and Peter Kroon, "Interoperability, switchability and portability: Implications for the cloud," Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, November 2022, https://www.econstor.eu/bitstream/10419/266527/1/1823592864.pdf; John Pendleton, Ariel Levite,Bob Kolasky, "Cloud Reassurance: A Framework to Enhance Resilience and Trust," Carnegie Endowment for International Peace, January 2024, https://carnegieendowment.org/2024/01/18/cloud-reassurance-framework-to-enhance-resilience-and-trust-pub-91394.

[79] Devika Narayan, "Platform capitalism and cloud infrastructure: Theorizing a hyper-scalable computing regime," Environment and Planning A: Economy and Space 54, no.5 (2022), https://doi.org/10.1177/0308518X221.

[80] Filippo G. Blancato, "The Cloud Sovereignty Nexus: How the European Union Seeks to Reverse Strategic Dependencies in Its Digital Ecosystem," Policy & Internet, 2023, https://doi.org/10.1002/poi3.358.

[81] Mariano-Florentino Cuéllar, The UK AI Safety Summit Opened a New Chapter in AI Diplomacy, Carnegie Endowment for International Peace, November 2023, https://carnegieendowment.org/2023/11/09/uk-ai-safety-summit-opened-new-chapter-in-ai-diplomacy-pub-90968.

[82] For detailed discussion, see James Shires, The Politics of Cybersecurity in the Middle East (London: Hurst, 2021).

[83] Robert Hannigan, "Organising a Government for Cyber", RUSI, 27 February 2019, https://www.rusi.org/explore-our-research/publications/occasional-papers/organising-government-cyber-creation-uks-national-cyber-security-centre.

[84] Office of the UN Secretary-General, "common Our Common Agenda: Report of the Secretary-General," 2021, https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf, 63.

[85] Pacte Numérique Mondial Contribution de la France, April 2023, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_France.pdf; Contribution to the Global Digital Compact of Switzerland, April 2023, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_Switzerland.pdf; and GDC Contributions of the Republic of El Salvador and the UK.

[86] Contribution of the Islamic Republic of Iran to the Global Digital Compact, April 2023, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_Islamic-Republic-Iran.pdf.

[87] Contribución de la República de Cuba al Pacto Digital Mundial, April 2023, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_Republica-de-Cuba.pdf.

[88] Ibid., 7.

[89] Contribution of the United Kingdom to the Global Digital Compact, April 2023, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_United-Kingdom.pdf, 3, 12.

[90] GDC Contribution of the Kingdom of the Netherlands, 8-9.

[91] Contribution of the European Union to the Global Digital Compact, March 2023, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_European-Union.pdf.

[92] Contribution of the European Union to the Global Digital Compact, 19.

[93] Ministry for Europe and Foreign Affairs of France, "Stratégie internationale de la France pour le numérique," December 2017, https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf, 20.

[94] Department for Science, Innovation & Technology (DSIT) and Foreign, Commonwealth & Development Office (FCDO) of the United Kingdom, "International Technology Strategy," March 2023, https://www.gov.uk/government/publications/uk-international-technology-strategy/the-uks-international-technology-strategy, 9.

[95] Department for Science, Innovation & Technology of the United Kingdom, "National Semiconductor Strategy," May 2023, https://web.archive.org/web/2/https://assets.publishing.service.gov.uk/media/646626780b72d3001334476d/national_semiconductor_strategy.pdf, 13-14.

[96] Ya-Wen Lei, The Gilded Cage: Technology, Development, and State Capitalism in China (Princeton, New Jersey: Princeton University Press, 2023).

[97] Elsa B. Kania, "Technology and Innovation in China's Strategy and Global Influence" in China's Global Influence: Perspectives and Recommendations, eds. Scott C. McDonald and Michael C. Burgoyne (Honolulu, Hawaii: Daniel K. Inouye Asia-Pacific Center for Security Studies, 2019), https://web.archive.org/web/20240215141922/https://apps.dtic.mil/sti/pdfs/AD1083478.pdf.

[98] David Gordon and Meia Nouwens, "The Digital Silk Road: China's Technological Rise and the Geopolitics of Cyberspace," International Institute for Strategic Studies, December 2022, https://web.archive.org/web/2/https://www.iiss.org/en/online-analysis/online-analysis/2022/12/digital-silk-road-introduction/; Jing Cheng and Jinghan Zeng, "Digital Silk Road" as a Slogan Instead of a Grand Strategy." Journal of Contemporary China, 2023.

[99] US Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014, https://web.archive.org/web/20240131190539/https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[100] James Shires and Isabella Wilkinson, "Selling digital insecurity," Chatham House, March 29, 2023, https://web.archive.org/web/20240214144440/https://www.chathamhouse.org/2023/03/selling-digital-insecurity.

[101] Pall Mall Process, "Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities," February 6, 2024, https://web.archive.org/web/20240215111239/https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.

[102] Ministry of Foreign Affairs of the Netherlands, "International Cyber Strategy 2023 – 2028" September 2023, https://www.government.nl/documents/publications/2023/09/12/international-cyber-strategy-netherlands-2023-2028, 13.

[103] European External Action Service, "2nd Foreign Information Manipulation and Interference Threats A Framework for Networked Defence," January 2024, https://web.archive.org/web/20240208184539/https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf, 6.

[104] Department of Foreign Affairs and Trade of Australia, "International Cyber and Critical Tech Engagement Strategy," April 2021, https://www.internationalcybertech.gov.au/sites/default/files/2021-05/21066%20DFAT%20Cyber%20Affairs%20Strategy%202021%20update%20Internals%201%20Acc.pdf.

[105] Smart Nation and Digital Government Office of Singapore, "Smart Nation: The Way Forward," November 2018, https://www.smartnation.gov.sg/files/publications/smart-nation-strategy-nov2018.pdf, 9.

[106] Ibid., 50.

[107] Office of the US President, 2020, 9.

[108] Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Strategy, White House, October 12, 2022, https://web.archive.org/web/2/https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/10/13/remarks-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-national-security-strategy/.

[109] Jill C. Gallagher, "U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests," Congressional Research Service, January 5, 2022, https://crsreports.congress.gov/product/pdf/R/R47012/2.

[110] Karen Freifeld, Alexandra Alper and Stephen Nellis, "U.S. stops granting export licenses for China's Huawei - sources," Reuters, January 31, 2023, https://www.reuters.com/technology/us-stops-provision-licences-export-chinas-huawei-ft-2023-01-30/.

[111] Office of the US President, 2020, 9.

[112] European Commission, "Joint Communication to the European Parliament, the European Council and the council on 'European Economic Security Strategy'," JOIN(2023) 20 final, June 2020, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0020&qid=1687525961309, 9.

[113] State Council Information Office of the People's Republic of China, "Jointly Build a Community with a Shared Future in Cyberspace," November 2022 http://english.scio.gov.cn/node_8033411.html.

[114] Ibid.

[115] Office of the President of the United States of America, "United States Government National Standards Strategy for Critical and Emerging Technology," May 2023, https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf.

[116] "Quad Principles on Critical and Emerging Technology Standards," Department of the Prime Minister and Cabinet of Australia, accessed on October 14, 2023, https://www.pmc.gov.au/resources/quad-principles-critical-and-emerging-technology-standards.

[117] European Commission, "European Economic Security Strategy," 9.

[118] Ibid.

[119] Tim Hickman and Detlev Gabel, Data Protection Laws and Regulations The Rapid Evolution of Data Protection Laws 2023-2024, International Comparative Legal Guides, July 2023, https://web.archive.org/web/20240215141444/https://iclg.com/practice-areas/data-protection-laws-and-regulations/01-the-rapid-evolution-of-data-protection-laws.

[120] Contribution of the Kingdom of the Netherlands to the Global Digital Compact, April 2023, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission-Kingdom-of-the-Netherlands.pdf.

[121] European Commission, "European Economic Security Strategy," 9.

[122] UK National Cyber Security Centre, "Guidelines for secure AI system development," November 2023, https://web.archive.org/web/20240211234756/https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development.

[231] Australian Cyber Security Centre, Engaging with Artificial Intelligence, January 2024, https://web.archive.org/web/2/https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/engaging-with-artificial-intelligence.

[124] NIS Cooperation Group, "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures," January 2020, https://web.archive.org/web/20240127145922/https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[125] European Commission, "European Economic Security Strategy," 14.

[126] Ministry of Foreign Affairs of Denmark, "Strategy for Denmark's Tech Diplomacy 2021-2023," February 2021, https://techamb.um.dk/strategy, 5.

[127] Ibid., 30.

[128] State Council Information Office of the People's Republic of China, "Jointly Build a Community with a Shared Future in Cyberspace," November 2022 http://english.scio.gov.cn/node_8033411.html.

[129] Department of Science and Technology of Iran, "Science, Technology and Innovation in Iran," January 2023, https://france.mfa.ir/files/frfrance/iran.pdf, 23.

[130] European Commission, "European Economic Security Strategy," 8.

[131] Ibid., 7.

[132] Council of the European Union, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND
OF THE COUNCIL establishing the Strategic Technologies for Europe Platform ('STEP') and amending Directive 2003/87/EC, Regulations (EU) 2021/1058, (EU) 2021/1056, (EU) 2021/1057, (EU) No 1303/2013, (EU) No 223/2014, (EU) 2021/1060, (EU) 2021/523, (EU) 2021/695, (EU) 2021/697 and (EU) 2021/241," 6378/1/23 REV 1, https://data.consilium.europa.eu/doc/document/ST-6378-2024-REV-1/en/pdf.

[133] European Commission, "European Economic Security Strategy," 8.

[134] European Parliament and of the Council, "Regulation (EU) 2023/2675 of the of 22 November 2023 on the protection of the Union and its Member States from economic coercion by third countries," Official Journal of the European Union.

About the authors

Max Smeets is the Co-Director of the European Cyber Conflict Research Initiative (ECCRI) and the European Cyber Conflict Research Incubator (ECCRI CIC). He is also a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich.

James Shires is the Co-Director of ECCRI and the European Cyber Conflict Research Incubator (ECCRI CIC). He is also a Fellow with The Hague Program on International Cyber Security.

Jakob Bund is a Senior Researcher in Cyber Conflict and Statecraft at ECCRI and an Associate at the German Institute for International and Security Affairs (SWP).

Acknowledgments

We would like to extend our gratitude to our colleagues at the Finnish Institute of International Affairs, KU Leuven, LUISS Guido Carli, and Maastricht University for enriching the research of the Work Package through their expertise and constructive collaboration. In particular, we are grateful to Joep Crompvoets, Roberta Haar, Dennis Redecker, and Paul Timmers for their careful review of this report and their thoughtful feedback. Any remaining mistakes or errors are the authors' alone.

Disclaimer

Funding for the research presented in this report was provided to ECCRI by UK Research and Innovation (UKRI), as a member of the consortium for the Horizon Europe project Reigniting Multilateralism Through Technology (REMIT). REMIT research is conducted under the umbrella of the European Union's Horizon Europe research and innovation program, grant agreement No 101094228. UKRI's and the European Commission's support to the project does not constitute an endorsement of its findings, which reflect the views of the authors alone. UKRI and the European Commission are not responsible for any use which may be made of the information contained therein.

About ECCRI

The European Cyber Conflict Research Initiative (ECCRI) promotes interdisciplinary research on cyber conflict and statecraft in Europe and beyond. Its mission is to make rigorous, objective research on these topics accessible to policymakers and the general public. ECCRI encourages and supports high-quality original research and helps researchers communicate their findings. It runs a wide range of initiatives, from a virtual research workshop series to the Oxford Cyber Forum. These events provide scholars and practitioners with a platform to discuss the latest developments in the field.

ECCRI is a UK Charitable Incorporated Organization. ECCRI's Registered Charity Number is 1190782.

Project background

Research for this report was conducted for the REMIT project "Reignite Multilateralism via Technology". Coordinated by Maastricht University, the REMIT project brings together leading European researchers from nine partners from Belgium, Estonia, Finland, Germany, Italy, the Netherlands, Romania and the United Kingdom.

REMIT aims to re-mobilize a transnational collective spirit that addresses global problems through technology. It seeks to develop a better understanding of the status quo, innovative methodologies, and policy recommendations that support effective policies to revitalize global democratic structures.,

ECCRI leads REMIT's research stream on the economic and societal factors that shape technology governance. Partners in this stream include the Finnish Institute of International Affairs (FIIA), KU Leuven, LUISS Guido Carli, and Maastricht University.

ECCRI EUROPEAN CYBER CONFLICT RESEARCH INITIATIVE

Maastricht University

KU LEUVEN

REMIT

FIIA
FINNISH INSTITUTE
OF INTERNATIONAL AFFAIRS

LUISS Università Guido Carli


ECCRI
EUROPEAN
CYBER
CONFLICT
RESEARCH
INITIATIVE