From Elements to Effects: The Strategic Imperative to Understand "*National Cyber Power*"

Carolyn Erickson and Matt Rasmussen
United States Army War College, Carlisle, PA, USA

carolyn.erickson@armywarcollege.edu
matthew.rasmussen.mil@armywarcollege.edu

Abstract: Increases in the use of Artificial Intelligence in industry, government, military, and daily life have brought cyber challenges and concerns to the fore. Each new development in disruptive technology broadens the attack surface for cyber-attacks and the necessity for cyber defense. The increased use of automation during and after the COVID-19 Pandemic has incentivized activity by state, non-state, and criminal actors in the cyber realm. An exponential increase in the use of Artificial Intelligence has brought along with it a requirement for data and energy for storage, access, and computing. Many nations have written strategic documents and strategies for dealing with national "cyber power", a term that is multifaceted and reaches beyond the traditional "cyber" realm. Current national cyber strategies over-emphasize cybersecurity and under-emphasize the structural elements behind cyber power, such as energy resources and data availability. Further, they are written to address one small aspect of national cyber power as defined by common indices, resulting in a fractured and de-synced national strategic approach to gaining national cyber power. In an era of AI ubiquity, strategic leaders need to make sound decisions about how to invest in the most critical areas to defend, maintain, and grow cyber power. Therefore, national cyber strategies should examine the full requirements for national cyber power. This paper will examine the critical components of a definition of "national cyber power" through a literature review of various national cyber security strategies and policy documents from various countries, think tank reports on cyber strategy, industry reports and white papers, and meta-analyses on cyber power and cyber capabilities. We examine the current and expected future trends in technology and how those are likely to shape the strategic environment. Finally, from this body of knowledge, we propose new considerations to retool strategic cyber documents.

Keywords: Cyber power, Strategy, Artificial intelligence (AI), Data, Energy

1. Introduction

National strategies allow states to codify principles, priorities, and tasks; they serve to define the strategic ends, ways, and means. National strategic documents set the boundaries and expectations for operational plans that follow. In the United States, the President's *National Security Strategy* sets the direction for the Secretary of Defense's *National Defense Strategy*, the Chairman of the Joint Chiefs of Staff *National Military Strategy*, and subsequent service documents.

As one example among many, the United States' *National Cybersecurity Strategy* focuses the United States government on five pillars: defend critical infrastructure; disrupt and dismantle threat actors; shape market forces to drive security and resilience; invest in a resilient future; and forge international partnerships to pursue shared goals (Biden 2023). This strategy pivots on two points: shifting cybersecurity responsibility off the end user and onto the network owners and operators and technology providers; and work to create market forces that reward security and resilience, focusing on resilience by design.

However, all current national cyber strategies over-emphasize cybersecurity and under-emphasize the structural elements behind cyber power, such as energy resources and data availability, while failing to synchronize with other critical pillars of national power that are measured by national cyber power indices. In an era of AI ubiquity, strategic leaders need to make sound decisions about how to invest in the most critical areas to defend, maintain, and grow cyber power. Therefore, national cyber strategies should examine the full requirements for national cyber power.

2. Literature Review

2.1 Defining "National Cyber Power"

The nuance between cyber and cybersecurity is meaningful when organizing a nation's finite and precious resources in a strategy to gain superiority. This section will reflect on common and military definitions of terms to help parse what constitutes cyberspace, what it means to secure it, what power is, and how one might possess cyber power.

The US military defines *Cyberspace* itself as a "global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the

Internet, telecommunications networks, computer systems, and embedded processors and controllers" (JP 3-12). Further, the military defines cyberspace security, or *cybersecurity*, as "actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation"(JP 3-12).

To frame the discussion of cyber power, it is useful to discuss power itself and look at other indices of national power developed before cyber was a consideration. Power has typically been defined as a nation's ability to achieve its strategic ends, and how to measure national power has been the subject of much study. Tellis (2000) focused national power measurement on national resources (ex. GDP), national performance (ex. infrastructure) and military assets (ex. Defense spending). A 2005 RAND conference report *Measuring National Power* (2005) provides this concept of national power: "State power can be conceived at three levels: (1) resources or capabilities, or power-in-being; (2) how that power is converted through national processes; (3) and power in outcomes, or which state prevails in particular circumstances." This definition is particularly helpful in thinking about the latent power of resources versus the active power of resources in action. Beckley (2018) posits that a nation's power has been poorly measured on gross (GDP, military spending) and a better prediction of a nation's power would be measured on net (GDP minus production, welfare and security costs), which he approximates with GDP x GDP per capita. Using the common metric for determining national power applied to national cyber power indicates that power is a function of GDP expense on cyber x GDP cyber per capita. By these metrics, a nation's investment in cyber as adjusted for population should indicate the more cyber powerful nation. Recently the University of Denver Korbel School's *Relative National Power Codebook* (2024) posits a metric of National Power that reflects the thoughts of Tellis and Beckly, and accounts for Military (personnel, spending, weapons), Human Capital, Economic (energy, GDP, and some factors of production), Technology and international interactions. However, national cyber power literature to date does not follow this model

As one looks at cyber power, it is helpful to think of the military's definition of *cyberspace superiority*, which is "the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force and its related land, air, maritime, and space forces at a given time and place without prohibitive interference" (JP 3-12). The IISS, in its *Cyber Power Matrix Overview*, defines *cyber power* as the ability of a state to project power in cyberspace, to achieve strategic objectives and exert influence globally" (IISS Cyber Power Matrix Overview 2024).

As nations attempt to gain, wield, and demonstrate their national cyber power, they often turn to national strategies to help organize their governments around their vision. A good strategy tells a story of national theory of victory that explains how the nation will design ways that use means to achieve its ends in the current situation with acceptable cost and risk. Strategy depends on the five elements of strategic logic: the situation; desired ends (objective); means to achieve those ends; designing ways to use the means to achieve the ends; and assessing costs and risks (Heffington 2019). This framework helps nations properly describe the environment and desired endstate, while organizing the whole-of-government around expending resources to reach the desired endstate. Given no nation has an infinite amount of people, money, or time, each strategy should discuss costs and risk of things left unaddressed due to lack of resources.

This paper will compare multiple current national cyber strategies against the two prevailing cyber power indices to see points of commonality, points of divergence, and further consider the impact of recent advances in AI on both the strategies and indices to recommend updated strategies for nation states to gain or improve national cyber power. This paper will further consider the RAND (2024) concept of national power to assess whether national cyber strategies are appropriately considering all factors of power (such as data and electricity) and how well nations are acting on their factors via strategies to generate national cyber power-in-action.

2.2 Major Components of Current National Cyber Strategies

A review of regional and national cyber strategies and nation-specific think tank reports across several nations in the IISS spectrum of cyber power tiers - Tier 1: US; Tier 2: UK, France; Tier 3: India, Japan (IISS 2021); and others: Singapore, Germany, Norway and the EU - revealed many common themes. The national cyber strategies and think tank reports reviewed had between three to five pillars. While each cyber strategy was organized differently and reflected the tenor of their national will, they all tended to share points of commonality in cybersecurity, technological advantage, governance, cooperation (internally to the country,

with other countries, and between public and private) and offensive cyber operations. By far the greatest emphasis was on cyber security and cooperation. Most governments mentioned the need for technological advantage and governance. Not all governments mentioned offensive cyber operations, but those who did were explicit in their desire to take down threat actors and prevent them from achieving their aims. Table 1.0 below lists these strategies with their pillars color coded to emphasize similar thematic elements.

Cybersecurity received the weight of discussion among the national strategies, with focus on protecting critical infrastructure. This theme overlapped heavily with the need for technological investment in resilient infrastructure, education, and a cyber-savvy workforce. Singapore was concerned with building resilient infrastructure (Loong 2021). India's think tank report mentioned cybersecurity in payments infrastructure and supply chains, reflecting unique concerns of their populace (Data Security Council of India 2020).

Governments were also concerned with maintaining a technological advantage, with focus on investment in the physical infrastructure and human capital pipeline. The EU focused on growing operational capacity to prevent, deter, and respond to cyber-attacks, but also technological sovereignty (European Commission 2020). Singapore made growing a robust talent pipeline a core pillar of their strategy (Loong 2021), while the UK made technological advantage a main pillar of its strategy. (HM Government 2022). India focused on strengthening its budget and research and development in the cyber domain (Data Security Council of India 2020). Governance appeared in several strategies, focused on how the government could shape market forces and work with others to set standards (a point where governance and cooperation overlapped in diplomacy). France was unique with one pillar focused on educating its citizens on appropriate cyber behavior (Valls 2015).

Cooperation was a strong topic of discussion, as nations variously combined and emphasized the need to cooperate internally in their government, externally with other nations and organizations, and between the public and private sectors. All nations sought to synergize within their nation, and most sought to develop shared goals with other like-minded nations to help influence the global commons on cybersecurity issues. Some nations with stronger divides between public and private sectors addressed the need for strong cooperation between the two. Norway's and Germany's strategy stood out for its strategy being cooperation focused across all its pillars (Norwegian Ministries 2019; Federal Ministry of the Interior, Building and Community 2021).

Offensive cyber operations were less discussed in national strategies. Some nations did not address the topic at all. Other nations spoke of cyber-crime investigation, others of disrupting and countering cyber threat actors. This mix of national strategy approaches likely reflects a combination of what the nation thinks is its government role and its capacity to engage in offensive cyber operations. The graphic below shows regional and national cyber strategies with their pillars color coded for common thematic elements. The EU is a Regional (R) strategy, with many National (N) strategies and several Think tank (T) strategies published by semi-governmental entities. The nation state and year of publication, if not in the title, is in brackets after the title. The pillars of each strategy have been sorted by theme. Each column represents a theme, to include: cybersecurity; public-private cooperation; technical and human investment; international cooperation; citizen wellbeing; and offensive cyber operations.

Table 1: National, Regional, and Think Tank Cyber Strategy Pillars Sorted by Common Theme

Name	Cybersecurity	Public-Private Partnership	Tech and Human Investment	International Cooperation	Citizen Wellbeing	Offensive Cyber
EU Cybersecurity Strategy (R) [2020]	Resilience, technological sovereignty and leadership		Operational capacity to prevent, deter and respond	Cooperation to advance a global and open cyberspace		
French National Digital Security Strategy (N) [2015]	Security of state and critical infrastructure	Private sphere, industrial policy export	Education	Europe, digital autonomy	Digital trust and privacy	
The **French** Approach to Cyber (T)[2023]			Competence (forward looking, operational efficiency, cyber training)	Openness to Traditional and New Partners (Europe, within the nation)	Agility (administration oriented on the beneficiary, experiment and innovate)	
Cyber Security Strategy for **Germany** (N) [2021]	Strong and sustainable cyber security architecture for every level of government	Government and private industry working together		Germany's active role in European and international cyber security policy	Remaining safe and autonomous in a digital environment	
India National Cyber Security Strategy 2020 (T)	Secure (critical infrastructure, payments, supply chain)	Synergize (standards, diplomacy, cybercrime investigation)	Strengthen (governance, budget, R&D)			
Cybersecurity Strategy [**Japan**] (N) [2015]	Safe and secure society - critical infrastructure protection		Cross cutting approaches - R&D, workforce	Peace and stability - national and international	Socio-economic vitality - Secure by design	
Norway National Security for Cyber (N) [2019]		Public-Private Partnership		International Cooperation		Civilian-Military Collaboration
Singapore Cybersecurity Strategy (N) [2012]	Build Resilient Infrastructure	Develop a Vibrant Cybersecurity Ecosystem	Grow a Robust Cyber Talent Pipeline	Enhance International Cyber Cooperation	Enable a Safer Cyberspace	
UK National Cyber Strategy (N) [2022]	Cyber Resilience		Technology Advantage	Global Leadership		Countering Threats
US National Cyber Strategy (N) [2023]	Defend Critical Infrastructure	Shape Market Forces to Drive Security and Resilience	Invest in a Resilient Future	Forge International Partnerships to Pursue Shared Goals		Disrupt and Dismantle Threat Actors

2.3 Major Components of "Cyber Power" Indices

The relatively limited number of comprehensive indices assessing "cyber power" reflects the complexity and novelty of measuring national power in the digital domain. The two prominent indices—the Harvard Kennedy School's Belfer Center's *National Cyber Power Index (NCPI) 2022* in the United States and the International Institute for Strategic Studies' (IISS) *Cyber Power and National Power: A Net Assessment*, an international think tank headquartered in the United Kingdom —emphasize different aspects of cyber power, which reveals important insights into why their authors prioritized certain elements over others.

First, the Belfer Center's NCPI emphasizes a multi-dimensional approach to understanding cyber power, recognizing that cyber capabilities extend beyond traditional security concerns. The index evaluates countries based on several categories: defense, offense, surveillance, control of the information environment, and economic strength in cyberspace. This broad approach reflects the growing importance of cyber power in all sectors of society—not just for defense or intelligence purposes, but also in terms of economic competitiveness and influence over the global information landscape.

The IISS reports, on the other hand, adopt a more traditional security-oriented approach. The two-part *Cyber Power and National Power: A Net Assessment* (2021, 2023) examines cyber power primarily through the lens of strategic competition, military capabilities, and intelligence-gathering potential. This reflects IISS's focus on national security and geopolitical stability, with the authors emphasizing cyber power as a key instrument of national power in a rapidly changing global security environment. The emphasis on military and intelligence capabilities can be attributed to the organization's defense and security focus, which naturally prioritizes how cyber tools can be leveraged in national defense, espionage, and in broader strategic competition among major powers. Recently, IISS has further developed their indices into a continually updated data set. The *IISS Cyber Power Matrix Dashboard* (2024) is a tool that tracks various aspects of state cyber power, including cyber operations, disinformation campaigns, and ownership of submarine cables. It compiles publicly available data on state-linked cyber activities and infrastructure to assess and compare the cyber capabilities of different nations. The dashboard is regularly updated to reflect new information and developments in the cyber domain and can be configured to view as a map, a timeline, or a network diagram.

The divergence in focus between these indices—one with a broader, multi-dimensional framework and the other with a security and military orientation—illustrates differing priorities in the conceptualization of cyber power. The Belfer Center's inclusion of economic and societal dimensions aligns with a recognition of the critical role of digital infrastructure in modern economies, reflecting the broader integration of cyber capabilities into national economic strategies. In contrast, the IISS's emphasis on military and intelligence capabilities underscores the strategic importance of cyber power in statecraft and global power dynamics, especially in an era of heightened cyber conflict and espionage. IISS's *Cyber Power Dashboard* is almost exclusively focused on cybersecurity with only one mention of critical infrastructure.

However, as we will describe below in future digital trends and implications, these indices come up short in understanding the substructures of cyber power. The indices focus on investment in the physical cyber layer and the personnel who conduct cyber offensive and defensive operations on the network, however they neglect the foundation upon which that network rests: electricity and data.

Points of Commonality and Divergence between Indices and Strategies with Implications

All cyber strategies mentioned the need for cyber defense (NCPI, IISS) for critical infrastructure, and many discussed the importance of economic strength in cyberspace (NCPI), especially in technology and building resilient infrastructure. Many reports at least inferred strategic competition (IISS) when addressing their need for cooperation with other nations or setting norms and standards in their strategies.

While many of the national cyber strategies covered national cyber power topics mentioned in the indices, there were clear lines of divergence. No national strategy mentioned surveillance (NCPI) or intelligence gathering (IISS), and many did not strongly focus on the information space (NCPI). Military capabilities in cyberspace (IISS) had very limited discussion, mostly aligned with national cyber strategies that mentioned offensive cyber operations against threat actors.

It is possible that nations chose to address all aspects of cyber national power, but in different strategies developed by separate organizations. If so, nations are making advances in each of those areas, but are at risk of decoupled and potentially conflicting strategies instead of building synergy across the cyber and information domains. Strategists must think more broadly about entities outside their control that could impact their

success and work to coordinate with them to at best work together for amplified effect, but at the least, avoid working counter to each other.

3. Anticipated Future Digital Trends and Implications

The emergence of OpenAI's ChatGPT in November 2022 significantly changed the landscape of the digital revolution. While not the first AI platform, this application sent shockwaves through the digital industry and pushed AI applications to the forefront of industry conversation. The ensuing clamor for all things AI has energized investment and development across industry for research and offerings

Increased AI investment is almost certain to continue in the near term. Around the world, most developed economies expect continued multi-billion dollar investment in AI development and systems through 2030 (Maslej 2024). The United States continues to be the global leader in AI investment, however, developing economies with large populations, such as India, are highly likely to increase demand on AI systems in those countries as adoption grows (Desislavov 2023).

It is almost certain that AI systems will continue to be used in cybersecurity operations in ever increasing density over the next 3-5 years (Camacho 2024). Machine learning (ML) and deep learning (DL) algorithms allow AI systems to become extremely adept in areas of threat detection, vulnerability assessment, and incident response (Sontan 2024). Because of this, government and industry use of AI is likely to continue to push investment beyond projected levels. It is highly likely that AI-enabled systems and operators will come to the fore in national and military offense and defense operations. Not only will criminal threats attempt to breach cybersecurity protocols, state and non-state actors will continue to conduct offensive cyber operations of increasing complexity against all types of targets using improved AI-enabled tools (Jun 2024).

Data is a vital resource for the continuing AI boom. Data feeds data-centric AI models; without trusted, cleaned, legal and ethical data it is likely that AI development will grind to a halt. The possibility of "model collapse" or "knowledge collapse" makes the issue of data supply and storage a more compelling strategic issue (Peterson 2024). Partial model collapse might make AI-enabled cyber systems less effective, damaging cyber offense or defense operations, thus driving governments to spend more resources to protect data.

Data centers have therefore become indispensable elements of contemporary digital infrastructure. In recent years, there has been a significant surge in data center construction, driven by the increasing demand for cloud services, artificial intelligence (AI), and data-intensive applications. The global data center market continues its rapid expansion into 2024, with ongoing investments and large-scale projects. This growth is not only quantitative but also qualitative, with notable increases in both hyperscale and edge data centers. Hyperscale facilities, operated by major companies such as AWS, Microsoft Azure, and Google Cloud, have proliferated, with over 1,000 such centers operating globally by early 2024. These facilities are characterized by their enormous energy consumption, often exceeding 100 megawatts. Concurrently, smaller, localized edge data centers are being developed to enhance data processing efficiency by reducing latency through proximity to end users. This expansion has also significantly increased energy consumption, with global data centers consuming approximately 220-250 terawatt-hours in 2022, according to the International Energy Agency (IEA, 2023).

The downstream effect of increased data, infrastructure, water, and energy requirements are likely to be reprioritization of adversary targeting. As governments and militaries look to AI-based solutions for warfare, the AI supply chain will become a target. Industrial targets have been seen as a lever for states to compel adversaries since the beginning of the 20th century. In particular, the development of the airplane, aerial warfare, and strategic bombing ushered in the era where a state's industrial base became seen as a valid target (Hoffman 2019). The efficacy of strategic bombing has been often debated since World War II to the present. However, one thing that is clear: states will target the sources of power of their opponent. Data centers, energy production and distribution facilities, water systems and telecommunications lines are likely to rise in priority as targets in an age of AI facilitated warfare (Anderson 2016).

This drastic change in the digital environment demonstrates the problem of narrowly focused cyber security strategies that do not take into account the substructures necessary for national cyber power. As one small example, while most nations have a Department of Energy developing various plans and strategies, they are separate from the cyber strategies the nation is developing except where cybersecurity of the energy infrastructure overlaps. Each group - energy and cyber - are developing their own strategies and plans, with the only cross talk of how whole-of-government approaches in one sector (the electric grid) impact the other sector (cyber power) is how to secure their grid against cyber-attack. The discussion is not about how the

energy strategy of the nation impacts its capacity for national cyber power. For instance, the US Department of Energy states in its 2022 Sustainability Plan that it is committed to transitioning from carbon sources of power to "clean" energy, while significantly increased demands for electricity from former gas sources (policy-induced gas-to-electric shifts in home heating, home cooking, and electric vehicles) (Department of Energy 2022) and exponentially increased AI power demands threatens to strain the power grid to collapse right when the nation may need to use its AI-enabled cyber power to advance or defend its national interests. Further research and discussion on this subject is warranted.

4. How Strategies need to Change

Current national cybersecurity strategies significantly undervalue the physical domain of data, infrastructure, and energy at the expense of discussing human capital, talent management, and commercial industry. To fully understand the requirements for national cyber power, strategic decision makers need to take all factors bearing on the problem into account. According to the RAND (2005) concept of national power, national cyber strategies are failing to account for factors of cyber power, such as data and electricity. Second, the isolated way in which various agencies who control those factors develop their strategies (ways to process those factors of power to create power-in-action) means that at the national level, those factors are not being thought of or acted upon in a synergistic way designed to maximize a nation's cyber power-in-action. In order to maximize national cyber power, the following changes must be made.

First, a comprehensive national digital strategy should address three additional fundamental categories: Data Supply and Storage, Physical Infrastructure, and Energy. The interdependence between these factors—data, infrastructure, and energy—will only increase, making it essential to integrate them into strategic frameworks. The substructures required for AI-enabled national cyber power are a critical part of the cyber ecosystem that must be addressed in a wholistic fashion to gain full advantage of synergy.

Second, national digital strategies must be better aligned with broader national security strategies. As nations increasingly depend on digital systems for critical functions—including military operations, national defense, and economic stability—there is a growing need to harmonize cybersecurity with broader defense and energy strategies. This would ensure that vulnerabilities in the digital domain do not become critical national security threats. Effective synchronization between these areas will also enhance resilience and ensure a more secure and reliable national infrastructure in the face of both cyber and physical threats.

One essential change in this approach is rethinking terminology. The term "cybersecurity" no longer captures the full breadth of the digital landscape. AI is just one aspect of a broader digital revolution that began with the rapid expansion of the internet in the 1990s and continues today. This revolution has transformed almost every aspect of society by making cyber-enabled systems ubiquitous. As AI, quantum computing, and other advanced technologies become more integrated, the physical components of the digital landscape—including data centers, energy consumption, and critical infrastructure—will grow in both relative importance and complexity. National strategies should reflect these shifts by adopting the term "National Digital Ecosystem Strategies" to represent not just cybersecurity, but the entire digital infrastructure on which modern states and economies rely.

5. Conclusion

Current national cyber strategies are siloed and do not fully address the pillars of national cyber power indices, nor the substructures critical to cyber capabilities in the AI-enabled world. National strategies must be updated in light of the environmental change brought by the advances of AI, address other elements of government and civil society that are critical elements of national cyber power, and truly encompass the entire digital ecosystem. Further study is warranted on the impact of AI's enormous energy requirements on government climate initiatives to decarbonize national power grids to avoid power grid insufficiency. National leaders need to recognize the different, cross-cutting elements and institute process and mechanisms to address through strategic documents.

Disclaimer: The views expressed are those of the authors and do not reflect the official policy or position of the US Army, Department of Defense, or the US Government.

References

Anderson, S. (2016) *Airpower Lessons for an Air Force Cyber-Power Targeting Theory*, [online], Air University Press, Maxwell Air Force Base, Alabama, Air Force, Cyber Power, Targeting: Airpower Lessons for an Air Force Cyber Power Targeting Theory (af.edu).

Beckley, M. (2018) "The Power of Nations: Measuring What Matters", [online], *International Security*, Vol 43, No. 2, pp 7-44, https://doi.org/10.1162/isec_a_00328.

Biden, J. (2023), *National Cyber Security Strategy,* [online], Washington, DC: White House, March, National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov).

Camacho, N. G. (2024) "The Role of AI in Cybersecurity: Addressing Threats in the Digital Age", [online], *Journal of Artificial Intelligence General Science (JAIGS)*, Vol *3, No.* 1, pp 143–154, https://doi.org/10.60087/jaigs.v3i1.75.

Data Security Council of India (2020) "National Cyber Security Strategy 2020", [online], 1664377398590fe3kyzt8xwd.pdf (cyberpolicyportal.org).

Department of Energy (2022) "2022 Department of Energy Sustainability Plan", [online], 2022_Sustainability_Plan_Final_Public_Release.pdf (energy.gov).

Desislavov, R., Martínez-Plumed, F. , and Hernández-Orallo, J. (2023) "Trends in AI inference energy consumption: Beyond the performance-vs-parameter laws of deep learning", [online], *Sustainable Computing: Informatics and Systems,* Vol. 3, https://www.sciencedirect.com/science/article/pii/S2210537923000124.

European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (2020) *EU Cybersecurity Strategy*, [online], The Cybersecurity Strategy | Shaping Europe's digital future (europa.eu).

Federal Ministry of the Interior, Building and Community (2021) *Cyber Security Strategy for Germany*, [online], https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-artikel.html.

HM Government (2022) "National Cyber Strategy 2022", [online], https://www.gov.uk/government/publications/national-cyber-strategy-2022.

Heffington, S., Oler, A., and Tretler, D. (2019) "A National Security Strategy Primer", [online], National Defense University Press, Washington, DC, 2019, A National Security Primer - National War College (ndu.edu).

Hoffman, A. (2019) "Systems Based Targeting", [online], University of New South Wales, Canberra, Australia, https://unsworks.unsw.edu.au/server/api/core/bitstreams/baacf111-297b-4169-89fa-f2d21b094b29/content.

IEA (2021) "Enhancing cyber resilience in electricity systems", [online], International Energy Agency, https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems.

IISS (2021) "Cyber Capabilities and National Power: A Net Assessment", [online], International Institute of Security Studies, Cyber Capabilities and National Power: A Net Assessment (iiss.org)

IISS Cyber Power Matrix (2024) "Cyber Power Matrix Overview", [online], International Institute of Security Studies, IISS Cyber Power Matrix: Overview.

Joint Chiefs of Staff (2022) *Joint Cyberspace Operations*, Joint Publication 3-12, Washington DC, Joint Chiefs of Staff, 2022.

Jun, J. (2024) "How Will AI Change Cyber Operations?", [online], War On the Rocks, April 20, 2024, How Will AI Change Cyber Operations? - War on the Rocks.

Kumar, S. Datta, V. Singh, S. K. Singh and R. Sharma, "Opportunities and Challenges in Data-Centric AI", [online], *IEEE Access*, vol. 12, pp. 33173-33189, 2024, Opportunities and Challenges in Data-Centric AI | IEEE Journals & Magazine | IEEE Xplore.

Loong,L.H. (2021) "The Singapore Cybersecurity Strategy 2021", [online], https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021.

Maslej, N., Fattorini, L.. Perrault, R. et al (2024) "The AI Index 2024 Annual Report", [online], Stanford University, HAI_AI-Index-Report-2024.pdf.

Moyer, J., Markle, A., Meisel, C. and Szymanski-Burgos, A. (2024). "Relative National Power Codebook, Version 10.07.2024.", [online], Frederick S. Pardee Institute for International Futures, Josef Korbel School of International Studies, University of Denver, https://korbel.du.edu/pardee/content/national-power.

Solberg, M. (2019), "National Cyber Security Strategy for Norway." [online], national-cyber-security-strategy-for-norway.pdf (regjeringen.no).

Peterson, A., (2024), "AI and the Problem of Knowledge Collapse", [online], forthcoming, [2404.03502] AI and the Problem of Knowledge Collapse (arxiv.org)

Sontan, A., Segun, S. (2024) "The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities", [online], *World Journal of Advanced Research and Reviews*, 2024, 21(02), 1720–1736, The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities (wjarr.com).

Tellis, A., Bially, J., Layne, C., and McPherson, M. (2000) "Measuring National Power in the Post Industrial Age", [online], RAND, Measuring National Power in the Postindustrial Age | RAND.

Treverton, G., Jones, S. (2005) "Measuring National Power", [online], RAND, Measuring National Power | RAND.

Valls, M. (2015) "French National Digital Security Strategy", [online], NCSS_FRANCE.pdf (itu.int).