Luiss
School of Government

Cyberspace Evolution and AI

The International Competition and the Regional Posture In GCC

Working Paper Series
SOG WP9/2024
ISSN: 2282-4189

Author: Luigi Martino
May 2024

LUISS

Table of Contents

1. Introduction

> AIs are imprecise, dynamic, emergent, and capable of "learning". AIs "learn" by consuming data, then drawing observations and conclusions based on the data.
>
> ***The Age of AI and Our Human Future***,
>
> H. Kissinger, E. Schmidt, D. Hutternlocher

The proliferation of Artificial Intelligence (AI) in our digital age is a direct consequence of the evolution of cyberspace. As the digital environment and technological landscape expand, they provide the infrastructure and data ecosystems essential for AI's development and deployment, transforming industries, economies, and social structures in deep ways. The relationship between technological advancements, increased data flows, and computational power in cyberspace has facilitated AI's rise and integration into various aspects of human activity. One of the primary catalysts for AI's growth is the exponential increase in data availability within cyberspace, and in particular the production and consumption of big data which become a cornerstone of modern AI[1]. This vast pool of data, generated by online activities, IoT devices, and specific characteristics of digital society, is crucial for training sophisticated AI models. These models learn and make predictions with unprecedented accuracy and speed, owing to the diverse and extensive datasets they process. The expansion of cyberspace is synonymous with enhanced computational resources: for instance, cloud computing platforms, provide necessary computational power and storage solutions at scale[2]. These platforms facilitate the deployment of complex AI algorithms that require significant computational power to efficiently process and analyse large datasets.

This accessibility to advanced computational resources from one side has democratized AI technology usage, on the other side has made them available to a few range of users and industries creating a differentiation in accessibility and control among the nations. At the same time, given that AI can be considered as the evolution of cyberspace's dynamics, new security challenges have emerged. As AI systems become more sophisticated, so do the cyber security threats aimed at exploiting them. These challenges underscore the need for robust AI security measures to prevent and mitigate risks, ensuring the safe use of AI technologies[3] and the capability form states to control these dynamics. A mirroring effect

[1] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt, 2013.
[2] DAVENPORT, Tara. Submarine cables, cybersecurity and international law: An intersectional analysis. Cath. UJL & Tech, 2015, 24: 57.
[3] SCHNEIER, Bruce. Artificial intelligence and the attack/defense balance. IEEE security & privacy, 2018, 16.02: 96-96.

of AI included in cyberspace dynamics is the lack of an internationally recognized and accepted regulatory framework able to govern the development and deployment of AI.

On one hand, governments and regulatory bodies are increasingly focused on creating frameworks that address concerns related to AI, such as privacy, surveillance, and ethical decision-making[4]. On the other hand, in the global AI race, states are trying to cover a pivotal role based on a dual capacity: able to face the confrontations inherent in international competition and technological challenges, while simultaneously being able to conceal strategic advancements and intentions to maintain a competitive edge[5].

This perspective is supported by H. Kissinger et al., who argue that current technological dynamics are not exempt from international politics; rather, technological confrontation is increasingly becoming a geopolitical issue characterizing the international arena of the 21st century[6]. The emergence of geopolitical dynamics within the context of developing technological competencies and controlling such technologies is marked by the novelty that states are not the only players in the arena. Another noteworthy element that characterizes the current digital society, a product of the information revolution[7], is the combination of three distinct characteristics that in different eras had never managed to merge into a single entity. Namely, the ability of technologies to be at the same time dual-use—thus usable both in military and civilian contexts; to be affected by rapid dissemination; and to possess a destructive potential. This triad of characteristics underscores the transformative impact of technology on global geopolitics and the strategic imperatives for state actors navigating this dynamic terrain at the global and regional levels.

This research aims to elucidate the strategic deployments of cyberspace within the complex matrix of global and regional dynamics, emphasizing the challenges and opportunities that arise as AI evolves. Notably, at the regional level, the case study will be focused on two major actors of the Gulf Cooperation Council (GCC) region, namely the United Arab Emirates (UAE) and the Kingdom of Saudi Arabia (KSA) where AI technology significantly influences regional power dynamics. The research will be structured around three pivotal sections.

The initial section (paragraphs 2 and 3) investigates the evolution of cyberspace and the power dynamics through the lens of the IR realist approach, with the main aim of answering the question of how major global powers are harnessing AI within the broader contexts of international politics.

The subsequent section (paragraph 4) focuses on the strategic deployment of AI by the UAE and KSA. It examines how these nations leverage AI to bolster their regional influence and economic diversification efforts. Through this analysis, the research seeks to provide a nuanced understanding of how AI, as a transformative element of cyberspace, is reshaping the dynamics of international relations and regional posture. Furthermore, the primary goal of this research is to substantially contribute to closing the knowledge gap surrounding this emergent topic, enhancing understanding of AI's impact on global and regional geopolitical frameworks.

[4] O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. Sci. Am, 2016, 315: 74-74.
[5] MARTINO, Luigi, "La guerra nel XXI secolo: la dimensione cyber e il conflitto russo-ucraino." In La guerra tiepida: Il conflitto ucraino e il futuro dei rapporti tra Russia e Occidente, edited by Andrea Manciulli & Enrico Casini. Koinè, 2023.
[6] KISSINGER, Henry A.; SCHMIDT, Eric; HUTTENLOCHER, Daniel. The age of AI: and our human future. Hachette UK, 2021.
[7] TOFFLER, Alvin. Future shock, 1970. Sydney. Pan, 1970.

2. Cyberspace at the intersection between politics and technology

The intersection of cyberspace with the political and technological landscapes presents a unique novelty that implies, inter alia, a re-assessment of the validity of the "classical" theoretical framework used in the past to describe the international relations paradigms. Cyberspace, originally a realm of pure technological development, has burgeoned into a critical arena of geopolitical contention that lacks predefined institutional hierarchies [8]. This evolution prompts two fundamental inquiries: firstly, the nature of structures, ***de facto*** hierarchies, and power dynamics that uniquely characterize cyberspace; and secondly, the extent to which the technological evolution of cyberspace is reshaping the power dynamics of international relations.

Joseph Nye[9] has been pivotal in addressing the politicization of cyberspace, suggesting that the diffusion of power is central to the cyber domain's role in international politics. Nye posits that cyberspace fosters a more distributed power landscape, potentially leading to a level playing field in international relations. However, contrary to Nye's more liberalist view, other scholars such as Carr[10], Martino[11], and Eriksson and Giacomello[12] present a realist perspective, arguing that the digital revolution is actually concentrating power in the hands of a few states and large corporations closely aligned with sovereign powers. This perspective is underscored by Henry Kissinger's (2011) proposal for a "cyber-détente" between the United States and China, advocating for a mutual recognition of cyber hegemony. In light of that, we can assume that the also in cyberspace there is an echo of Kenneth Waltz's view of international politics as a domain "without a system of enforceable laws". According to this perspective, cyberspace (in an analogous way to the international system) operates in an environment without a centralized hierarchical authority, leading to a complex structuring of power hierarchies.

However, the classical equation of international relations equal states, which is used by realist authors such as Waltz, in cyberspace is affected by the role of non-state actors and their role of champions as well as technological gatekeepers. Regarding this latter point, which includes, for instance, the power detained by the private actors to deny or allow access to the data managed by global platforms (such as social media), as suggested by Kissinger et. al.[13] "[...] because the governments generally do not create or operate these network platforms, the actions of inventors, corporations and individual users will shape the field along with government restrictions or incentives, creating a strategic arena that is particularly dynamic

[8] CHOUCRI, Nazli. Cyberpolitics in International Relations. The MIT Press, 2012.
[9] NYE, Joseph. The Future of Power in the 21st Century. Public Affairs Press, 2011.
[10] CARR, Madeline. (2017). "Cyberspace and International Order." DOI: 10.1093/oso/9780198779605.003.0010. Pages 162–178
[11] MARTINO, Luigi, "Cyber diplomacy e relazioni internazionali: le iniziative diplomatiche per mitigare il rischio di escalation militare nel cyberspazio," In Il ruolo dell'Italia nella sicurezza cibernetica. Minacce, sfide e opportunità, edited by Valerio De Luca, Giulio Terzi di Sant'Agata & Francesca Voce, 2018.
[12] ERIKSSON, Johan; GIACOMELLO, Giampiero. Space and the New Iron Curtain. Crisis Response Journal, 2022, 7.3: 84-85.
[13] KISSINGER, Henry A.; SCHMIDT, Eric; HUTTENLOCHER, Daniel. The age of AI: and our human future. Hachette UK, 2021.

and difficult to predict"[14]. Consequently, given that governments typically neither develop nor directly manage the fundamental components of cyberspace, including advanced realms like artificial intelligence, the configuration of this digital ecosystem is predominantly shaped by the initiatives of non-state actors, notably corporations. These actors, through their profit posture and innovation-oriented agenda, interact with government entities, introducing a layer of dynamism and inherent unpredictability into the international politics domain. Indeed, this complexity is further compounded by the diverse interests and strategies of these various stakeholders, each of whom brings unique influences that shape the trajectory of technological development and regulation.

The inherent risks associated with these power dynamics are not only observed in traditional domains such as military or economic spheres but are also prevalent in the cyber domain where they are less visible and harder to quantify. The digital age has lowered barriers to ICT development and complicated the cyber environment, particularly concerning anonymity, thus exacerbating issues of trust, transparency, and security among states. From a systemic viewpoint, cyberspace has altered the mechanisms of power exercise, enabling both state and non-state actors to extend their influence and strategic objectives globally. This new form of cyber power plays a crucial role in shaping political decisions, alliances, and conflicts within the international system. Considering Waltz's systemic conception of international relations, cyberspace contributes to a decentralized, anarchic, and highly interconnected political landscape, where mutual adaptability is necessary. The theory of complex interdependence, as elaborated by Nye and Keohane[15], is particularly relevant in understanding the cyber arena. This theory, based on multiple, non-hierarchical interactions across various issues, finds a distinctive echo in cyberspace, where interactions are characterized by a variable geometry of connections that intertwine the physical and virtual layers of existence. However, these connections, influenced by political dynamics, often exacerbate the security dilemma—a core element in the study of international relations.

The digital age might thus be seen as a period not of power diffusion, as some have predicted, but rather as one where power is increasingly concentrated in the hands of technologically capable states and entities. This paradoxical development suggests that despite the potential for a more interconnected and dependent world, the dynamics of cyberspace may instead drive states towards strategies that prioritize national security and self-help, reinforcing the security dilemmas posited by realists like Waltz (1979) and Hertz (1981).

[14] Ibid.
[15] NYE, Joseph S.; KEOHANE, Robert O. Power and interdependence. World Politics in transition, 1977.

3. Is Cyber Power a Real Power?

The conceptualization of power is the subject of extensive discussion in the field of International Relations theories[16]. As outlined by the realist school of thought, power holds significant importance in shaping both peace and conflict in the international arena[17]. Within the classical realist framework, global politics revolves around a contest for power among nation-states, a perspective reiterated by Morgenthau when he posits, "Whatever the ultimate aims of international politics, power is always the immediate goal"[18]. Neo-realists assert that power serves as a means through which states ensure their survival within an anarchic international system, devoid of a dominant authority capable of ensuring harmonious and coordinated coexistence[19].

According to this approach, power is conceived in terms of a combination of resources and goods (elements of national power) possessed by a country[20]. In this regard, Morgenthau provides various material elements of power, such as geography, natural resources, and military strength, as well as immaterial elements like national character (including morale) and the quality of governance[21]. Similarly, Waltz lists among the elements involved in defining a nation's power: population, territory, natural resources, economic capability, and military strength, along with political stability and the competence of a state[22]. In line with this tradition of thought, Mearsheimer conceptualizes power exclusively as the material capabilities of the state, arguing that power simply represents "specific goods or material resources available to the state"[23].

The alternative school of thought, opposed to the realist approach, is predominantly represented by authors who argue that power does not manifest through resources, but rather through relations and interactions among social, institutional, or economic actors. According to this relational approach, power is defined as the ability to influence and control others. Similarly, Nye, through a liberal institutional approach, argues that "the test of power lies not in resources, but in the ability to change the behaviour of states," specifying that hard power is combined with the concept of soft power capable of shaping the preferences of other states so that they voluntarily change their behaviour through a kind of moral persuasion rather than coercion[24].

[16] GUZZINI, Stefano. On the measure of power and the power of measure in International Relations. DIIS working paper, 2009;
[17] ARON, Raymond. Main Currents in Sociological Thought, Vol. 2. New Brunswick. NJ: Transaction Books. HANDBOOK OF PUBLIC ADMINISTRATION, 1970, 22: 26-34.
[18] MORGENTHAU, Hans; NATIONS, Politics Among. The struggle for power and peace. Nova York, Alfred Kopf, 1948.
[19] WALTZ, Kenneth N. Theory of international politics, Berkley University Press, 1979
[20] MORGENTHAU, Hans; NATIONS, Politics Among. The struggle for power and peace. Nova York, Alfred Kopf, 1948.
[21] Ibid.
[22] WALTZ, Kenneth N. Theory of international politics, Berkley University Press, 1979
[23] MEARSHEIMER, John J. The tragedy of great power politics. WW Norton & Company, 2001.
[24] NYE, Joseph S. Soft power. Foreign policy, 1990, 80: 153-171.

Aside from the theoretical speculations of the aforementioned authors, at a pragmatic level, in the search for a conceptual framework of power that boasted both epistemological rigour and pragmatic utility for this research, we can turn to Dahl's formulation, which portrays power as an innate construction intrinsic to human actions, appearing more appropriate [25]. Dahl's perspective posits power as an intrinsic constituent of social and political dynamics, involving a spectrum of actors (individuals, groups, governments, and nation-states) engaged in its exercise. Dahl underscores power through a bidirectional dynamic between actor A and actor B. According to Dahl: A has power over B to the extent that A can get B to do something that B otherwise would not do[26].

Correspondingly, Carr - who is known as the pioneer in systematically clarifying power through a realist framework - highlights the broader conceptualization and divergent manifestations of power, each delineated by specific spheres of application conditioned by social relations. Carr postulates that power operates to influence actors' ability to shape their own "destiny." In this sense, as Carr argues, power assumes multifaceted forms, conditioned by the nuances of the political and social environments in which it is exercised [27]. In light of Carr's theory of power, Barnett and Duvall [28] assert that the multiple conceptualizations of power are not only discrete but also intimately intertwined, influenced by the context in which power dynamics develop.

Therefore, it can be assumed that power in international relations emanates from an actor's ability to strategically allocate their resources for the pursuit of their goals in opposition to another actor's preferences. In accordance with the conventional interpretation of power - particularly as supported by the realist paradigm within IR, adopted in this research for its ability to comprehend both tangible and intangible dimensions of power - power entails the ability of international political actors to leverage diverse heterogeneous resources as intrinsic state goods such as territory, population, raw materials, military and economic wealth, and, last but not least, also immaterial resources like human morale and civil-military technological capabilities.

At this point, the need arises to delve into the level of analysis regarding the capacity or lack thereof to quantify and qualify the cyber power of a given actor. In theory, it should not be difficult to identify actors, assess their importance, even in quantitative terms, and analyse their interactions in terms of exchange, cooperation, competition, conflict, control capability, and dependency within cyber dynamics. However, a thorough analysis of the cyber domain reveals how uncertainty and the intrinsic military use capacity of civilian tools contribute to creating serious doubts about the possibility of adopting the "old rules" of legal and military limits on violence in a dimension where the concept of war is based on the "virtualization and anonymization" of conflicts.

Indeed, it is no coincidence that from an operational standpoint, according to the National Military Strategy for Cyber Operations of 2006 (NMS-CO), the cyber environment can be described through the acronym VUCA: Volatility, Uncertainty, Complexity, Ambiguity. More specifically, the cyber environment is subject to constant, increasingly rapid changes over time, making it extremely volatile (V); consequently, we are faced with a high degree of uncertainty (U) due to the impossibility of fully understanding it and predicting the nature or effects of these changes. Furthermore, being a highly complex system (C), i.e.,

[25] DAHL, Robert A. The concept of power. Behavioral science, 1957, 2.3: 201-215.
[26] Ibid.
[27] CARR, Edward H. The Twenty Years' Crisis (second edition, London), 1949)
[28] BARNETT, Michael; DUVALL, Raymond. Power in international politics. International organization, 2005, 59.1: 39-75.

formed by an interaction between various systems, it is impossible to know all the interactions between its parts, leading to ambiguity (A) in its interpretation, as the known parts are insufficient to understand the system. All this makes it difficult to quantitatively classify a concept that qualitatively remains nuanced or rather "below the threshold" of the use of force.

Indeed, as Nigel Inkster[29] has observed: "The evolution of the cyber domain [...] has significantly complicated this situation, not only in terms of how armed forces adopt and adapt to new technologies but also in raising questions about what constitutes military use in a domain where civilian and military users are inextricably intertwined, and where many cyber capabilities that are not military in nature can be used to generate effects that are militarily significant".

We have chosen to align the measurement of cyber power by embracing Dahl's definition of power, according to which: "the capacity of A to induce B to do what B otherwise would not have done," as it provides the foundations for measuring cyber power. Indeed, this definition implies that both state and non-state actors can exercise coercive power since "multinationals can use their control over capital to shape foreign [and global] economies" and "networks and non-state groups sometimes [...] terrorize entire populations."

In particular, Dahl's conception of power does not require an exclusive recourse to material resources but also includes symbolic and normative resources[30]. In addition to these elements, there is another peculiar characteristic of power: dominance. Let's consider the concept of dominance, which we can define as "overwhelming superiority"[31]. This will not be achieved in cyberspace, unlike the terrestrial, maritime, aerial, and space domains, where military dominance can be reasonably achieved. In cyberspace, this exclusive dominance cannot be attained due to three key characteristics: the number of players, the easily accessible use of tools, the barrier to entry of violence and "territory," and the possibility to act anonymously.[31] Therefore, by combining this conceptualisation of cyber power, we have chosen to apply two primary conceptual approaches that have been identified in Table 1: the perspective of cyber power as resources and the perspective of cyber power as outcomes.

Cyber power approach	**Observable actions**
Cyber Power as Resources (***Cyber power understood as an actor's resources invested in its cyber posture and as a resource to achieve goals***)	Cyber expenditures Cyber offense Cyber defence Cyber operations Cyber deterrence Cyber-attacks and counter attacks capabilities Cyber intelligence, military and national bodies; Capacity building projects

[29] INKSTER, Nigel. The Huawei Affair and China's technology ambitions. Survival, 2019, 61.1: 105-111.
[30] VAN HAASTER, Jelle. Assessing cyber power. In: 2016 8th International Conference on Cyber Conflict (CyCon). IEEE, 2016. p. 7-21.
[31] Ibid.

	Propaganda and Soft Power usage International Partnerships Investments Standards and economic banning capabilities Personnel officially dedicated to cyber operations.
Cyber Power as Outcomes ***(Cyber power understood as outcomes, that is, the ability of one actor to influence the preferences of other actors)***	Diplomatic initiatives and results of negotiations Interpretation and applicability of International Law; Influence on international agenda Multistakeholders and Multilateralism debate Shifting national & global political dynamics.

Table 1. Different conceptualisation of cyber power

The first level of analysis, known as "power as resources," assesses cyber power based on the resources (human, technological, military, etc.) invested by a country in its cyber posture. This approach considers that wealth (thus investments and expenditures) enables a country not only to exercise its technological and human capabilities to enhance its defensive and offensive posture but also to gain influence through economic assistance, and investments, and thus exert soft power by financing global propaganda campaigns, organizing international events and capacity-building programs, or sponsoring advanced research projects in the context of relevant technology transfer. Military resources, such as the presence of dedicated cyber operations commands, allow a country to both exercise its hard power by creating a deterrent force against enemies and weaker countries and form alliances based on mutual defence.

The second approach, namely "power as outcomes," conceptualizes cyber power primarily as a matter of outcomes, such as an actor's ability to prevail in a dispute, set the agenda for international negotiations, or influence the preferences of other countries. This approach requires the observation of international events, such as military operations, large-scale cyberattack campaigns, or diplomatic negotiations, to determine the extent to which participants have influenced outcomes according to their interests.

Following the conceptualisation of power (Table 1) and its interrelation with exercise tools (provided by van Haaster[32]), we can attempt to structure a general taxonomy of cyber power as described in Table 2. These two analytical and conceptual approaches to cyber power can be integrated with the use of four classical power tools that, as highlighted by van Haaster[33] although there are semantic nuances among the power tools exhibited by actors in international politics, these tools can be considered foundational to the use of cyber power by any state or non-state actor aiming to have a significant role in cyberspace.

[32] VAN HAASTER, Jelle. Assessing cyber power. In: 2016 8th International Conference on Cyber Conflict (CyCon). IEEE, 2016. p. 7-21.
[33] Ibid.

Cyber Power as	*Levers of Cyber Power*	
	Political	**Economical**
Resource	• Orchestrate coordination through state like-minded • Employ social media platforms to legitimize actions • Employ cyber capabilities as deterrents, such as leveraging zero-day vulnerabilities, malware, and retaliatory measures • Utilize cyber capacities for international interventions (Stuxnet and NotPethya) • Influence, propose or ostracize diplomatic initiatives	• Safeguard domestic industries or acquire competitive insights • Establish national authority over cyber security • Provide financial or material assistance to other entities or actors (e.g., network infrastructure support, cpapcity building support) • Affect financial market technologies (e.g., targeting SWIFT network).
	Information	**Military**
Outcomes	• Influence both domestic and international target audiences through strategies like social media manipulation • Form target audiences' perceptions through information campaigns • Validate domestic actions and undermining foreign actions through social media platforms • Employ cyber capabilities for defensive purposes, including intrusion detection systems (IDS), intrusion prevention systems (IPS), and similar measures • Employ cyber capacities for intelligence purposes, such as surveillance and data collection	• Engage in overseas intervention based on full spectrum dominance or multidomain operations using military cyber capabilities • Attain authority over critical infrastructure (e.g., customized access). • Shape actors' behavior through deterrence strategies (e.g., showcasing cyber capabilities and red lines). • Impede, interrupt, weaken, or dismantle infrastructure (e.g., DDoS attacks, malware). • Conduct information campaigns targeting specific audiences (e.g., through social media or fake news campain).

Table 2. A Taxonomy of Cyber Power[34]

According to this taxonomy, the political tool encompasses the field of internal governance and external diplomacy, while the informational tool concerns activities aimed at disseminating, acquiring, protecting, and monitoring information. At the same level, the economic tool involves the use of financial means and economic strategies to exert influence on other actors, and the military tool serves as an extension of foreign policy, exercised both coercively (hard power) and persuasively (soft power). Additionally, to these four tools, other civilian capabilities include legal authorities, law enforcement, administrative bodies, education, healthcare, public service providers, etc[35].

Cyber power is thus correlated between two intrinsic dimensions: the classification of resources and means through which power is exercised (i.e., levers), and the particular attributes of these resources in terms of their capacity to generate effects and outcomes.

Practically, on one hand, the "power as resources" approach is one of the most popular practices in "measuring" state cyber power. Over the years, many tools have been employed to measure the use of cyber power to extract the posture of state actors[36], their readiness, and their preparedness, even globally categorizing cyber forces[37] with a focus on the purposes of some countries over others. At the same time, measuring "power as resources" has two main limitations: the inability to reliably attribute cyberattacks and the difficulty of measuring resource capabilities by extrapolating data not only from government budgets but also including observed variables of resources made available by private actors or criminal

[34] Authors' Elaboration based on VAN HAASTER, Jelle, 2016.
[35] VAN HAASTER, Jelle. Assessing cyber power. In: 2016 8th International Conference on Cyber Conflict (CyCon). IEEE, 2016. p. 19.
[36] VOO, Julia, Irfan Hemani and Daniel Cassidy."National Cyber Power Index 2022." Belfer Center for Science and International Affairs, Harvard Kennedy School, 2022.
[37] VALENTINO-DEVRIES, Jennifer; YADRON, Danny. Cataloging the world's cyberforces. The Wall Street Journal, 2015, 11.

groups that may provide (and in cyberspace sometimes are constant) their services to states to achieve political-military objectives.

On the other hand, the "power as outcomes" approach identifies "who" has achieved "what," "when," and "how" in a specific issue, also explaining cases where the less-resourced party has succeeded. For example, this approach is useful for measuring cyber power in the Russo-Ukrainian conflict from 2014 to 2022, during the annexation of Crimea and after its large-scale invasion.

Here, it is possible to verify how, in the first case (time interval 2014-2021), Russia was able to use cyber power to achieve significant operational results, as it happened in 2014 through disinformation campaigns in Ukraine. At the same time, the most evident result obtained by Russian cyber power was in 2015 when, through a systematic campaign of cyberattacks perpetrated by pro-Russian groups, it was possible to cause a blackout in the energy transmission system over a large part of Ukrainian territory[38]. The same approach can be used to measure the cyber influence power exercised in international contexts of cyber diplomacy, testing, for example, the ability of certain countries to influence negotiation outcomes in different forums. A practical example of this observation derives from the ability of the Russian Federation to have influenced both the dynamics of negotiations at the United Nations (e.g., in 2017 with the refusal to approve the UNGGE report and the creation in 2019 of the OEWG duplicating activities within the UN context) and in the OSCE where, at the time of writing this article, the approval of new Confidence Building Measures (CBMs) is blocked on how international law applies in cyberspace[39]. This Russian capability also reflects the posture of the United States, which, through soft power, has been able to build a series of alliances (like-minded states) to counter the Russo-Chinese approach on one hand and strengthen the capabilities of weak allies like Ukraine on the other. However, the "power as outcomes" approach also has some weaknesses that limit its utility in empirical studies of international politics. For example, as Beckley observes, it is difficult to know the preferences of many countries in hundreds of events over time, making it difficult to objectively assess power.

According to the taxonomy provided in Table 2, our hypothesis is that an appropriate framework for measuring cyber power should incorporate two intrinsic dimensions: the categorization of resources and levers through which power is exercised, and the specificity of these resources regarding their ability to produce results on actors' cyber capabilities. Given this reasoning, we can contemplate a series of indicators to quantify cyber power, starting from observations within the domain of investments in the development and deployment of technologies which also include, inter alia, the AI domain.

.

[38] JASPER, Scott. Russian Cyber Operations: Coding the Boundaries of Conflict. Georgetown University Press, 2022.
[39] MARTINO, Luigi. "Le iniziative diplomatiche per il cyberspazio: punti di forza e di debolezza." IAI Papers, no. 21/13. Published by Istituto Affari Internazionali, 2021.

4. The super-power confrontation and the risk of securitization of AI

The escalating competition between the United States and China, along with conflicts in Europe and the Middle East, and shifting global alliances have culminated in what Cohen et al.[40] describe as the most unstable geopolitical period since the Cold War and the most significant innovation since the internet: the rise of generative artificial intelligence. The release of tools such as Large Language Models (LLMs), starting with the first version of ChatGPT in 2022, illustrates how the technological revolution and geopolitical tensions of the 21st century have intersected distinctly. Indeed, the concept of cyberspace has traditionally been viewed as a domain for interaction between human and computer elements. However, the advent of LLMs marks a paradigm shift towards human-computer integration, with generative AI becoming a central component, characterized by user interfaces that are common, proficient, and easily identifiable. Unlike previous technological revolutions – from the printing press to the internet – policymakers have had simultaneous access to these new technological capabilities (i.e. generative AI based on LLMs) culminating in the fastest adopted technology in history. With its widespread adoption and the acceleration of innovation, we have entered what Cohen et al. [41] terms the "inter-AI years" a period during which nations are assessing how to leverage opportunities while mitigating risks. In this context, as shown by Figure 1, the global interest in AI is also represented by various legislative and regulatory actions approved by countries between 2016 and 2023.

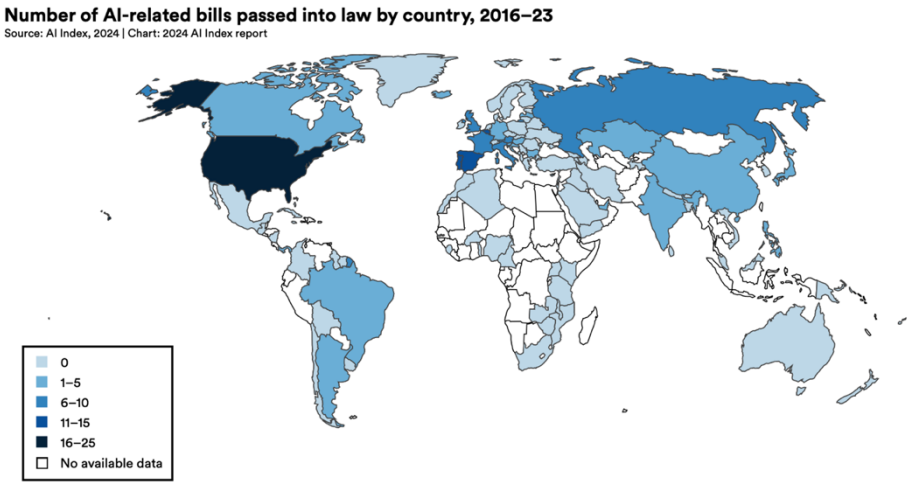

Figure 1. Number of related bills passed into law by country[42]

[40] COHEN Jared, LEE George, The generative world order: AI, geopolitics, and power, Goldman Sachs, 2023
[41] Ibid.
[42] STANFORD, Artificial Intelligence Index Report, 2024

Alongside global policy initiatives, the race for technological supremacy AI between the United States and China transcends economic boundaries, delving into political and military dimensions. Schmidt [43] highlights that by 2022, the interaction between these nations in AI will have increasingly incorporated strategic considerations affecting national security and geopolitical dynamics. A significant milestone was marked in 2022 when the Defense Advanced Research Projects Agency (DARPA) successfully tested an AI bot piloting an F-16 fighter jet in Southern California, underscoring the extensive nature of the AI race that extends beyond tech giants to include national governments.

This scenario epitomizes the deepening global competition in AI, amid rising geopolitical tensions between the U.S. and China, where AI technologies are not merely tools of innovation but pivotal elements in strategies for global dominance. This competition also manifests in the form of technological exchanges across borders, similar to the divisions seen with the internet, which have led to restrictive measures such as China's limitations on local companies supporting services like ChatGPT, and the U.S. amplifying export controls on AI technologies to China[44]. Such developments could push both nations towards more isolated technology development paths, potentially leading to a state of technological autocracy.

Moreover, the battle for AI dominance does not present a straightforward winner-takes-all scenario. For instance, China's advantage in facial recognition technology, bolstered by its authoritarian disregard for privacy, is countered by the stifling of innovation in other AI areas like linguistic models under the same regime, potentially placing China at a strategic disadvantage compared to more open societies such as the U.S.[45]. The competition extends to securing strategic resources essential for AI development, such as cutting-edge computing technologies, vast data repositories, advanced algorithms, and specialized expertise, crucial for nations to not only develop but also integrate AI into their broader economic and military frameworks.

This intricate interplay of innovation, policy, and competition emphasizes the multifaceted nature of global AI development, where technological progress is deeply intertwined with strategic geopolitical interests, shaping the future landscape of international relations and technological confrontation. The perception of this competition may also enhance the "securitization" perspective in AI, similar to the earlier militarization of cyberspace. In this respect, Schmidt stated that: "Only the United States and China have the resources, commercial might, talent pool, and innovation ecosystem to lead the world in AI. In some areas of AI research and application, China is a peer, and in certain applications, China is already more technically advanced. Within the next decade, "China could surpass the United States as the world's preeminent AI power"[46]. Furthermore, in the context of the ongoing rivalry for AI supremacy between the United States and China, a common narrative among U.S. policymakers has been the assumption that China's spending on AI, particularly for military purposes, far exceeds that of the U.S. This perception has raised concerns about the U.S. potentially falling behind, thereby threatening its technological and democratic leadership. However, research conducted by the Center for Security and Emerging Technology suggests that China's actual investment in AI may be less than the perception of the U.S. [47], with a

[43] SCHMIDT, Eric. AI, Great Power Competition & National Security. Daedalus, 2022, 151.2
[44] STANFORD, H. A. I. Stanford institute for human-centered artificial intelligence, 2020.
[45] MARTINO, Luigi, "La guerra nel XXI secolo: la dimensione cyber e il conflitto russo-ucraino." In La guerra tiepida: Il conflitto ucraino e il futuro dei rapporti tra Russia e Occidente, edited by Andrea Manciulli & Enrico Casini. Koinè, 2023.
[46] SCHMIDT, Eric. AI, Great Power Competition & National Security. Daedalus, 2022, 151.2: p. 288
[47] WEINSTEIN, Emily S.; LUONG, Ngor. US Outbound Investment into Chinese ai Companies. Center for Security and Emerging Technology, 2023.

significant portion of funds allocated to non-military initiatives such as basic algorithm research, robotics, and smart infrastructure development (see the figure 2).

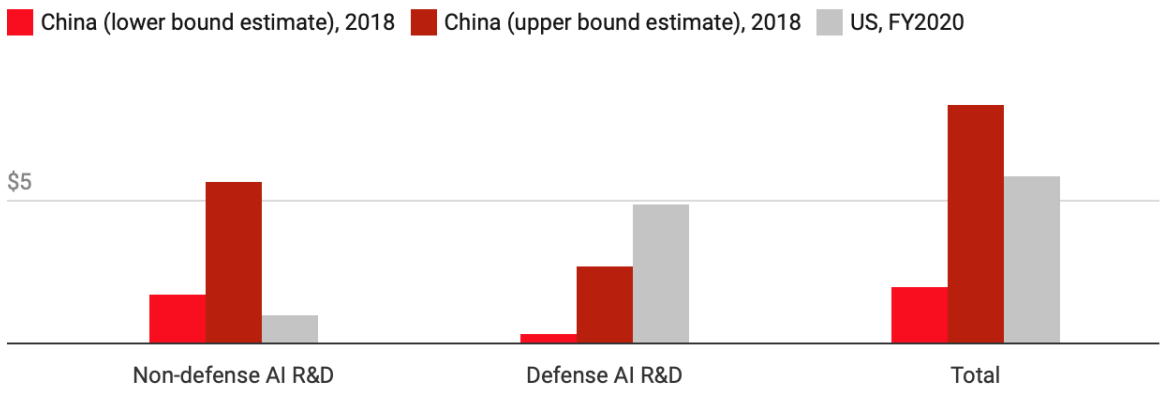

Figure 2 How the Chinese and US governments compare in terms of AI spending in billions[48]

Contrastingly, the U.S. has designated a substantial portion of its AI Federal budget towards defence for the fiscal year 2020, emphasizing its strategic priority in maintaining the technological edge in military applications.

Furthermore, a 2022 report from Stanford University positions the United States and China as the top two nations in terms of total private investments in AI.[49] However, as shown in Figure 3, from 2013 to 2021, U.S. private investments in AI have been three times higher than those made by China, highlighting a significant American lead in private sector AI funding.

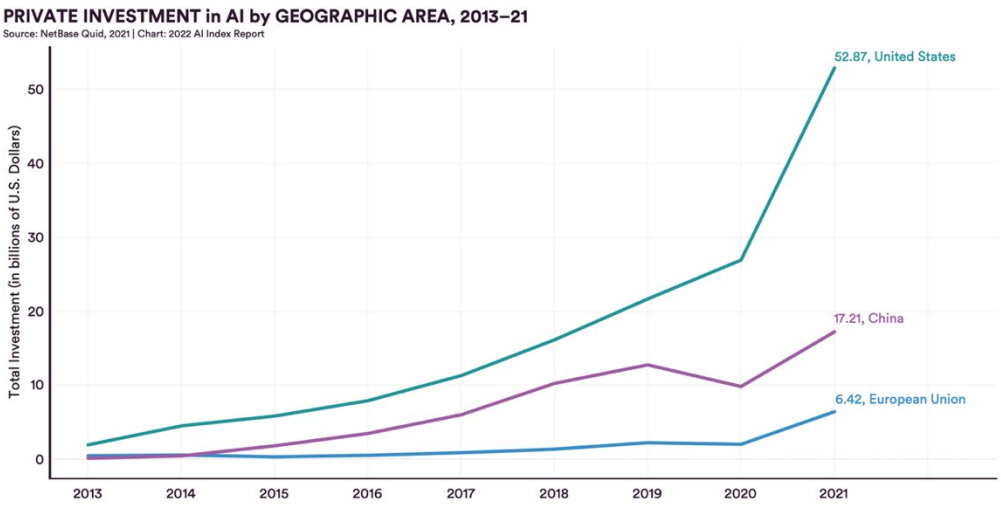

Figure 3 Private Investment in AI by Geographic Area[50]

[48] HAO, Karen. Yes, China is probably outspending the US in AI—but not on defense. MIT Technology Review. Accessed May, 2019, 11: 2020.

[49]

[50] ZHANG Daniel, Nestor Maslej, Erik Brynjolfsson, John Etchemendy, Terah Lyons, James Manyika, Helen Ngo, Juan Carlos Niebles, Michael Sellitto, Ellie Sakhaee, Yoav Shoham, Jack Clark, Raymond Perrault, "The AI Index 2022 Annual Report," AI Index SteeringCommittee, Stanford Institute for Human-Centered AI, Stanford University, March 2022.

This nuanced understanding of AI investment trends between the U.S. and China demonstrates the complex, multifaceted nature of the competition, where direct comparisons may not fully capture the strategic allocations and priorities of each nation.

The allocation of budgets for AI development carries significant political implications: the notable disparity in AI investment highlights the pronounced commitment of the U.S. to advancing AI technologies in comparison to its global counterparts, in particular, compared to China. In addition, this different posture also accentuates the relatively minor competitive stance of the European Union in this arena, reinforcing its identity as a regulatory power.

At the political level, if we agree to consider the proliferation of AI as a natural extension of the evolution of cyberspace, the expansion of AI capabilities in the near future will raise concerns about the use of force within the cyber domain. This development mirrors the historical progression seen with cyber weapons and will likely intensify discussions about AI arms control and the broader securitization of AI policies. Mügge[51] and Burton[52] noted that this shift towards framing peace within the logic of war invites a Foucauldian analysis, exploring the profound integration of militaristic logic within technological advancements that are ostensibly aimed at peace.

[51] MÜGGE, Daniel. The securitization of the EU's digital tech regulation. Journal of European Public Policy, 2023, 30.7: 1431-1446.
[52] BURTON, Joe. Cyber security. In: Research Handbook on NATO. Edward Elgar Publishing, 2023. p. 267-279.

5. The Global Impact of Cyberspace and the Regionalization of AI: the case of UAE and KSA

While the United States and China dominate the AI field, the broader cyber ecosystem and technological development within the ICT context are both global and regional in scope. Nations such as India, Israel, Singapore, South Korea, Japan, the United Kingdom, and France are considered mid-power players in the AI arena. This dynamic is part of what has been termed "the era of AI nationalism"[53] indicating that the benefits of specific AI investments by countries will have both national and regional impacts.

As highlighted by Berggruen and Gardels[54], AI has emerged as a formidable resource that will shape the destiny of nations going forward. While the full future impact of AI remains unpredictable, it is evident that a nation's geopolitical positioning and its capabilities in AI are becoming increasingly intertwined. This correlation is particularly evident in countries like the United Arab Emirates (UAE) and Saudi Arabia (KSA), which are investing heavily in developing technological capabilities and national champions in AI. These investments are part of a broader strategy to secure a sustainable future beyond their traditional reliance on limited natural resources such as oil. In this regard, the geopolitical aspirations of these countries are closely linked to their capabilities in AI, positioning them to potentially achieve regional mid-power status similar to the aforementioned countries as described in Figure 4.

Figure 4. AI-related investments pledged by governments[55]

[53] DHABI, Abu et al., Welcome to the era of AI nationalism, The Economist, 2024
[54] GARDELS, Nathan; BERGGRUEN, Nicolas. Renovating democracy: Governing in the age of globalization and digital capitalism. Univ of California Press, 2019.
[55] DHABI, Abu et al., Welcome to the era of AI nationalism, The Economist, 2024

According to Figure 4, in 2023 six governments worldwide – Great Britain, France, Germany, India, Saudi Arabia, and the United Arab Emirates – pledged to collectively invest approximately $40 billion in artificial intelligence (AI). A considerable portion of this investment is targeted towards acquiring graphics processing units (GPUs), which are crucial for training AI models, and constructing facilities to produce these chips (Economist 2024).

In the case of KSA and the UAE, they are leveraging their positions as "oil nations" to supply the necessary GPUs and the substantial energy required for these power-intensive chips, aligning with their R&D-oriented policies towards AI and ICT in general. Investments are also channelled into developing human capital: Universities in these two countries, such as Khalifa University of Science, Technology and Research and the Mohamed bin Zayed University of Artificial Intelligence in Abu Dhabi, along with the King Abdullah University of Science and Technology in Saudi Arabia, have been able to attract distinguished professors from world-renowned universities like MIT, UC Berkeley, and Carnegie Mellon University. A significant number of their students and researchers are international, many of whom choose to stay in the region after graduation. The AI ecosystems in the UAE and Saudi Arabia are particularly ***sui generis*** because they effectively integrate public, academic, and private sectors, to create extensive economic spillover effects[56]. For example, the UAE Technology Innovation Institute's Falcon model, an open-source AI initiative, aims to distribute AI benefits within the UAE across both public and private sectors. This model also seeks to attract international expertise and investment and compete with global AI models like Llama2 developed by Meta. In 2024, the UAE launched AI 71, a company aimed at commercializing AI research projects like Falcon and enhancing its open-source models using national datasets from various sectors[57].

Additionally, in 2023, Saudi Arabia initiated a significant $100 billion fund to invest in AI and other technologies. This was recently demonstrated at GAIA, an artificial intelligence start-up accelerator, for which Saudi officials last month announced funding of $1 billion. Each start-up participating in the program receives a grant of approximately $40,000 in exchange for a minimum three-month stay in Riyadh, along with a potential investment of $100,000. Entrepreneurs are required to register their company in the kingdom and spend 50% of their investment in Saudi Arabia. They also receive free access to computing power purchased from Amazon and Google. Approximately 50 start-ups from Taiwan, South Korea, Sweden, Poland, and the United States have participated in the GAIA program since its inception last year. This initiative is part of Saudi Arabia's broader strategy to cultivate a thriving AI ecosystem by attracting global talent and fostering technological innovation within the kingdom. This academic approach aligns with the nation's economic diversification goals under Vision 2030, leveraging its substantial financial resources to build a competitive edge in the global technology landscape[58].

Considering these substantial investments in both economic and human capital, it can be argued that the two case studies - UAE and KSA - represent significant developments in the dynamics of regional AI capabilities. This is evident from both an economic perspective, as well as in terms of their capacity to

[56] BARTENSTEIN, Ben. UAE poised to exit watchdog's dirty money list after reforms, MoneyWeb, 2024.
[57] Ibid.
[58] SATARIANO Adam, MOZUR Paul. 'To the Future': Saudi Arabia Spends Big to Become an A.I. Superpower, NYTimes, 2024.

pursue national technological autonomy. Indeed, the research suggests that, within the framework of competition between global superpowers, UAE and KSA are strategically developing their technological and research capacities in AI. Their objective is twofold: firstly, to establish a competitive stance independent from the primary global competitors, and secondly, to diversify away from their dependence on oil—a finite natural resource—thus aiming to achieve a stature of regional power within the Middle East. This strategic direction reflects a broader commitment to redefining their economic bases and enhancing their geopolitical influence through advanced technology, positioning themselves as pivotal players in the regional and global AI landscape.

6. Conclusions

The proliferation of Artificial Intelligence (AI) within our digital age marks a significant evolution of cyberspace, transforming industries, economies, and social structures profoundly. As the digital environment expands, it provides the necessary infrastructure and data ecosystems for AI's development and deployment. The relationship between technological advancements, increased data flows, and computational power in cyberspace has facilitated AI's rise, integrating it into various human activities. The accessibility to advanced computational resources, such as cloud computing, instead of democratizing AI technologies, making them available to a broader range of users and industries, is creating differentiation in accessibility and control among nations. Furthermore, the expansion of AI capabilities has also introduced new security challenges. Indeed, the lack of an internationally recognized regulatory framework to govern AI development and deployment further complicates the landscape of competition between two major actors such as China and the U.S. Moreover, given the global AI race, states are trying to cover a pivotal role, facing confrontations inherent in international competition and technological challenges while simultaneously concealing strategic advancements to maintain a competitive edge. The emergence of geopolitical dynamics within the context of developing technological competencies and controlling such technologies marks a novel aspect where states are not the only players. This mirrors the dynamic nature of cyberspace, which, originating from the information revolution, combines dual-use technologies, rapid dissemination, and destructive potential that underscores the transformative impact of technology on global geopolitics. This research has tried to elucidate the strategic deployments of cyberspace within the complex matrix of global and regional dynamics, emphasizing the challenges and opportunities that arise as AI evolves. Notably, the UAE and KSA, are emerging as AI significantly influencer middle-powers in the regional dynamics. The strategic use of AI by these nations not only enhances their geopolitical standing but also supports their economic diversification efforts away from oil dependency. The evidence emerged from the two case studies conducted to explain how AI, as a transformative element of cyberspace, is reshaping the dynamics of international relations and regional posture.

Acknowledgements

Il presente paper è stato realizzato nell'ambito del progetto "Geopolitica del Digitale", promosso dalla Fondazione Med-Or, in collaborazione con il Center for International and Strategic Studies (CISS) della Luiss Guido Carli, grazie al sostegno della Fondazione Compagnia di San Paolo all'interno del bando "Geopolitica e tecnologia".

About Luiss School of Government

The Luiss School of Government (SoG) is a graduate school training high-level public and private officials to handle political and government decision-making processes. It is committed to provide theoretical and hands-on skills of good government to the future heads of the legislative, governmental and administrative institutions, industry, special-interest associations, non-governmental groups, political parties, consultancy firms, public policy research institutions, foundations and public affairs institutions. The SoG provides its students with the skills needed to respond to current and future public policy challenges. While public policy was enclosed within the state throughout most of the last century, the same thing cannot be said for the new century. Public policy is now actively conducted outside and beyond the state. Not only in Europe but also around the world, states do not have total control over those public political processes that influence their decisions. While markets are Europeanised and globalised, the same cannot be said for the state.

The educational contents of the SoG reflect the need to grasp this evolving scenario since it combines the theoretical aspects of political studies (such as political science, international relations, economics, law, history, sociology, organisation and management) with the practical components of government (such as those connected with the analysis and evaluation of public policies, public opinion, interests' representation, advocacy and organizational leadership).

For more information about the Luiss School of Government and its academic and research activities visit. www.sog.luiss.it

Luiss
School of Government

Via di Villa Emiliani 14
00197 Roma
T +39 85 225052
sog@luiss.it