Chinese Political Science Review
https://doi.org/10.1007/s41111-024-00248-0

ORIGINAL ARTICLE

China as a Threat and Balancing Behavior in the Realm of Emerging Technologies

Maria Papageorgiou[1] · Muhammed Can[2,3] · Alena Vieira[2,3]

Received: 15 February 2023 / Accepted: 25 January 2024

Abstract

In the last years, China and the United States of America (US) have engaged in unprecedented competition in emerging technologies (ETs), in a context of China's growing presence and shifting position in the international system. Drawing on data between 2017 and 2023 and strategic decisions, such as bans and export controls directed at China's companies and the changing alignment posture of Western states, we employ the Balance of Threat (BoT) theory to examine China's changing aggregate power, offensive capabilities and aggressive intentions, while also establishing the vanishing importance of the geographic dimension. We then turn to the behavior of the US and Western states by drawing on the BoT theory, which suggests balancing as a prime strategy to counter the threat and identify instances of the formation of a balancing coalition against China. We demonstrate how the notion of threat in ETs can be approached and conclude with a characterization of balancing in the domain of ETs that resonates with the notion of "gradual balancing", in addition to outlining suggestions for future studies.

Keywords Balance of threat · Balancing · Emerging technologies · China · Threat · Alliances · Artificial intelligence

1 Introduction

The exponential growth of emerging technologies (ETs),[1] including 5G networks, Big Data, quantum computing, and artificial intelligence (AI), demands a reassessment of the role of technology in international affairs and its impact on the

[1] Emerging technology refers to an entity whose effects are still potentially available or under development that might bring about breakthroughs in the technology realm (Rotolo et al. 2015).

✉ Maria Papageorgiou
maria_marypapageorgiou@hotmail.com

[1] University of Exeter, Exeter, UK

[2] University of Minho, Braga, Portugal

[3] CICP/University of Minho, Braga, Portugal

Published online: 10 April 2024

international system. Control over ETs is no longer limited to the private sector, having become "the new strategic national security fulcrum of the 21 century" (You 2021). This heightened sensitivity toward ETs arises chiefly from the unpredictable implications these technologies pose for national security, as well as their potential impact on shifting the Balance of Power due to the economic and military advantages they confer (Steff et al. 2020). And while ETs on the whole have been viewed as potential game changers in military and strategic affairs, resulting in a securitization of the high-tech sector (Sechser et al. 2019; Huang and Mayer 2023), special attention has increasingly been paid to China's technological advancements and assertive technology policy through such initiatives as Made in China 2025, Next Generation Artificial Intelligence Development, and Digital Silk Road Project (under the Belt and Road Initiative).[2]

Assessed alongside their international economic, geopolitical and military developments, and despite their limitations, China's technological advancements have led to a widely circulated assumption that China is seeking to challenge the United States' (US) global primacy (Allisson 2017; Eslami et al. 2023; Heath et al. 2021). As a result, China has been viewed as a strategic competitor of the US and a growing threat (in US and other countries),[3] a notion that proliferated under the Trump[4] administration, with its emphasis on decoupling in the technological domain, and has continued during the Biden administration.[5] The resulting heightened competition, reflected in the new "Tech Cold War" (Bremmer and Kupchan 2018; Culpan 2019; Wu et al. 2019) and "AI Arms Race" debates (Pecotic 2019; Scharre 2019), has characterized the relationship between China and the US ever since.

China's advancements in the domain of ETs could conceivably equate to the acquisition of new capabilities, thereby inducing threat perceptions among other global actors. This corresponds to the realist perspective of international affairs: the US views its hegemony as increasingly challenged vis-à-vis a rising China that could adopt an ambitious strategy with escalating demands, thereby threatening a declining state's vital interests and raising the potential for conflict (Mearsheimer 2015; Shifrinson 2018). The designation of China's ET advancements as a threat, and their implications, deserves systematic academic engagement and theory-informed analysis. Two issues that remain unanswered in spite of the dynamically growing research

[2] This is in addition to the 13th 5-Year National Science and Technology and Innovation Plan (2016), Action Framework for Promoting Big Data (2015), Internet Plus (2015), or the Artificial Intelligence 3-year Action and Implementation Plan (2016).

[3] China has been referred to as an "epoch-defining and systemic challenge with implications for almost every area of government policy and the everyday lives of British people" (Integrated Review Refresh 2023, 30), and a "competitor and systemic rival" (Germany's National Security Strategy, 2023), in addition to the 'de-risking approach' adopted by the EU (Huang and Slosberg 2023; Campion 2020).

[4] The National Strategy for Critical and Emerging Technologies (2020) has recognized China's "pursuit to become the global leader in S&T" (2020, 1), and the notion of China as a threat has gathered broad bipartisan support.

[5] The National Security Strategy (2022) has referred to an outright competition and significant threats coming from China, as it "is using its technological capacity and increasing influence over international institutions to create more permissive conditions for its own authoritarian model, and to mold global technology use and norms to privilege its interests and values" (23).

field of ET studies are: What constitutes a threat in the context of ETs and how does China fit within these criteria? And, once a state is recognized as a threat, how do other states respond? Indeed, one could argue that state behavior and patterns of alignment in ET make an interesting case for thinking through the applicability of various International Relations (IR) theories and reassessing the existing analytical tools.

The state-of-the-art on ETs includes several important contributions, such as exploring the securitization act in the context of US–China overall competition (Moore 2023) from a securitization studies perspective. Given that ETs have been characterized as a critical frontier for national security and development, several scholars have examined how China's advancements have raised concerns among other countries (Kania 2022), with China perceived as a technological threat and an existential challenge to the Western way of life (Zhang 2021). Others have explored security discourses on critical infrastructure, especially with regard to companies like Huawei or ZTE (Campion 2020), in addition to exploring China's ascent as a science and technology powerhouse with its growing influence on the global stage (Segal 2019).

While the well-documented competition between the US and China has garnered significant attention (Yilmaz and Sun 2023; Khan 2021), particularly in the realm of ETs (Lee 2024; Christie et al. 2023; Harwit 2023), scholarly works have homed in on specific technological domains (Rim 2023; Wang and Chen 2018; Alderman and Ray 2017). China's aspirations to dominate information and communications technologies (ICT) and related fields such as AI have further underscored its material capabilities and modernization initiatives (Inkster 2019). Especially relevant to the present research are those studies that have focused on the US and the competition in ETs as a threat to its hegemony (Xin 2021) and assessed the implications of the US–China ET rivalry for the international system (Sun 2019; Montgomery 2017; Wu 2020; Can and Kaplan 2020) by employing the Balance of Power theory and relating the idea of threat to the distribution of power capabilities (Jensen et al. 2020; Horowitz 2018; Haas and Fischer 2020; Fischer and Wenger 2021; Ayoub and Payne 2016; Williams 2019). This is in addition to more recent contributions that have employed the BoT theory to carry out a quantitative assessment of responses to the Huawei ban as indication of response to a threat (Christie et al. 2023). Finally, scholars have explored the stances of other international actors and whether they perceive China as a threat in light of their strategic behavior (Shah 2023; Christie et al. 2023; Saltzman 2023; Papageorgiou and Melo 2022; Can and Kaplan 2020), focusing on US allies in Asia, namely, Australia, Japan, and South Korea as they have navigated expectations of mutual support from Washington in the process of decoupling Chinese technology companies from global supply chains (Lee et al. 2022) while also evaluating how the ET competition has affected alliance dynamics (Payne 2018; Corcoral 2021), the notion of extended deterrence and strategic stability (Mehta 2021). Relatedly, Friis and Lynsle (2021) have distinguished between an approach of "macrosecuritization" of China by the US and a securitization limited to specific domains like 5G technology (termed "niche securitization").

Aiming to contribute to these dynamically growing research fields, the present paper attempts to address two existing shortcomings. First, existing studies have often explored particular strategic decisions targeting Chinese companies (such as the Huawei bans). Second, the notion of China as a threat was mostly examined by focusing on aggregate power, even though supplemented by the analysis of pre-existing ideas among the US and its allies (Lee 2023), culture, geography (Payne 2018), and the political rhetoric and ideological tensions between China and democratic/pro-Western Asian countries (Salzman 2023; Mascitelli and Chung 2019), including the idea of a potential democratic anti-China coalition amidst the escalating technology race (Grotto and Schallbruch 2019; Scott and Bordelon 2023). A systematic, theory-informed analysis of what constitutes a threat in the context of ETs, especially including an unraveling of its individual components and how China fits these criteria, remains missing. Given the importance of ETs for a new distribution of power in the international system, it seems imperative to turn to theories capable of accounting for the respective dynamics.

We turn to Walt's Balance of Threat (BoT) theory and adopt the associated quadripartite definition of what constitutes a threat and the proposed responses to it. The BoT theory, with the power distribution in the international system at its core, is especially relevant to the objectives of this paper, aimed toward examining the "game-changing" potential of ETs, while also "understand[ing] a number of events that we cannot explain by focusing solely on the distribution of aggregate capabilities" (Walt 1987, pp. 263–264). In this perspective, China's growing ET power is a threat that urges states to (re)consider their balancing options. The latter may vary in intensity and assume different manifestations: first, diplomatic and policy coordination among competitors of the threat; second, the adoption of bans and restrictions/export controls aiming to undermine a rival's power; and third, strategic alignment excluding or targeting the threat and stating a clear objective of targeting its advancements in the ET domain. All the outlined options include accepting and aligning with the recommendations made by the US, particularly those aimed at countering Chinese initiatives in ETs (Christie et al. 2023). We, thus, turn to a Neorealist IR approach, applying it to a recent, multifaceted, and dynamically changing international phenomenon of ETs. The plausibility probe of the BoT theory, a stage of inquiry preliminary to the testing aimed at probing the plausibility of specific hypotheses/assumptions (Eckstein 1975), is carried out by analyzing the available statistical data from different sources, ranging from market shares to budget expenditure, and key strategic decisions, including the export restrictions, bans, and the changing alignment options of Western states, between 2017 and 2023.

We begin by presenting this study's theoretical framework and demonstrating how the notion of threat in ETs can be approached by considering the BoT theory's quadripartite approach, while also showing the vanishing relevance of the geographic dimension and laying out state strategies to counter the threat in the form of (external) balancing. We demonstrate China's growing threat in the ET domain assessed through aggregate power by focusing on AI, quantum computing and Big Data, China's offensive capabilities (corresponding to the civil-military fusion) and China's aggressive intentions (reflected in its covert operations). We continue by laying out state strategies to counter the threat in the form of balancing and identify manifestations of balancing behavior as a response to China's ET threat on the part of Western states between 2017 and 2023. We conclude with the characterization of balancing in the domain of ETs, which resonates with the notion of "gradual balancing," and outline suggestions for future studies.

2 Balance of Threat Theory and Balancing Behavior in the ET Domain

Threat plays a crucial role in shaping state behavior, according to BoT theory (1987), which considers that a state's aggregate power (total resources), as well as its geographic proximity, offensive capabilities, and aggressive intentions constitute the elements of threat, without providing guidance on how they are prioritized: "one cannot determine a priori … which sources of threat will be most important in any given case; one can say only that all of them are likely to play a role." (ibid, p. 26).

Consequently, and first, the states with a significant number of material capabilities, whether in military, economic, land, or population, signal a threat to others and the greater the aggregate power, the greater the threat a state can pose (Walt 1987). Due to their rapid evolution, ETs may extend into areas of especial importance for state survival, including intelligence, warfare, and critical infrastructure protection (Scharre 2023). The evolution of AI, Big Data, quantum computing, and IoT has the potential to rapidly transform the capabilities of nations and introduce new elements of power. The advancement in these ETs can be assessed by diverse indicators that capture their level of development, including its many attributes, expressed, inter alia, in relevant index rankings, number of patents or market share.

The second element of the BoT theory, geographical proximity and geography in general, has been linked with a propensity toward international conflict, particularly between neighboring countries (Bak 2018; Starr 2005; Buzan 1991). According to Walt (1985, p. 10), "the ability to project power declines with distance, states that are nearby pose a greater threat than those that are far away". The distance that lies between potential competitors limits "the ability to project power" and automatically makes the potential threat less intense (Walt 1987, pp. 21–26). However, in the ET domain, threats are not constrained by geographic boundaries as they originate from anywhere, unimpeded by traditional air, land, or sea defenses. Indeed, ETs such as AI, have become crucial to the control of geographic space and the five dimensions of warfare (land, sea, air, space, and cyber) and their interoperability (Fricke 2020), and it is the transboundary nature of ETs that makes detection and attribution more challenging.

Moreover, and third, states with large offensive capabilities, which refer to their capacity to threaten the sovereignty of other states, pose a greater threat compared to states with primarily defensive capabilities. According to Walt, "offensive power is also closely related but not identical to aggregate power" and corresponds to the ability to "threaten the sovereignty or territorial integrity of another state at an acceptable cost" (1987, p. 24). This element describes the material capabilities that can be used to initiate an attack related to military power. Offensive capabilities in military armament have defined the power competition among states, both in the quantity of armament and in technological advancement. In the ET domain, offensive capabilities can be assessed through military–civil fusion, given its implications for the rate of military technological diffusion and the offense–defense military balance (Lobell

2018). The rates of technological diffusion are associated with important military innovations that reinforce the threatening component of a rival's power (Can and Vieira 2022; Goldman and Andres 1999; Adams 2003).

The fourth and last element, aggressive intentions, is perceived as more threatening by those seeking to maintain the status quo (Walt 1988). It is based on the notion that "states that are viewed as aggressive are likely to provoke others to balance against them" (Walt 1987, p. 25). As such, "if a state is believed to be unusually aggressive, potential victims will be more willing to use force to reduce its power, to moderate its aggressive aims, or to eliminate it entirely" (Walt 1987, p. 19). Walt considers that "aggressive intentions" are equal to or override capabilities when estimating threats given that "perceptions of intent are likely to play an especially crucial role in alliance choices." (1987, p. 25).

Aggressive intentions are the most undertheorized element in Walt's theory and the most difficult to both conceptualize and operationalize—and, arguably, the most important in the constitution of threat. For instance, in AI, malign usage of technology is still a complex phenomenon that might disrupt every walk of life while progression in AI might extend the scale of existing threats, introduce new threats or change typical characteristics of threats in digital, political, and physical security (Brundage et al. 2018). Aggressive intentions focus on perceptions of malevolent intent; in this case, whether the state under suspicion *really does have aggressive intentions* is irrelevant; what matters is how those intentions are perceived and evaluated by other states. In this regard, in the domain of ETs, covert operations such as cyberattacks, espionage, and misinformation are of special importance as assessments of each state's intentions and motivations to use ETs. These attacks are not limited to extracting strategic information, including espionage in national defense and military intelligence fields, but also include the use of Internet bots to spread disinformation and influencing information narratives in various aspects of the targeted society. Our take on aggressive intentions sees the use of covert operations to conduct espionage, surveillance, or cyberattacks with the intent to gather sensitive information, undermine security, or disrupt critical infrastructures while AI propaganda and influence operations such as AI-powered algorithms, bots, or deepfakes to spread disinformation, manipulate public opinion, and influence political, social, or economic outcomes in a manner that serves aggressive or destabilizing goals that pose risks to the national security of states (Table 1).

2.1 Balancing Behavior in the ET Domain

When faced with a threat, states in an anarchic international system can either balance the threat or bandwagon with the source of the threat. Balancing, also defined as "a countervailing policy designed to improve abilities to prosecute military missions in order to deter and/or defeat another state" (Elman, 2003, p.8), indicating that "alignment[6] against the threatening power to deter it from attacking or to defeat

[6] Walt (1987) uses the terms "alignment" and "alliance" interchangeably, referring to both formal and informal arrangements.

Table 1 Elements of threat in ETs. *Source*: Authors' compilation

Elements of threat in BoT	Manifestation in ET	Areas/examples
Aggregate power	Advancements in strategic ETs	AI, Big Data, quantum computing, Internet of Things, semiconductors
Geographical proximity	Transboundary application	–
Offensive capabilities	Technological advancements in the military to threaten national security	Military–civil fusion
Aggressive intentions	Covert operations	Cyberattacks, political espionage, disinformation, bots and intellectual property theft

it if it does"[7] (Walt 1988, p. 278). According to BoT theory, both external balancing and bandwagoning rely on alliances, which Walt defines as "formal or informal arrangements of security cooperation between two or more sovereign states" (Walt 1987, p. 1).

Both the BoT and other contributions agree on the different intensity of balancing. According to the former, the intensity of the balancing behavior may depend on the level of threat and the certainty about the identity of the main threat (Walt 1992). Other authors consider balancing as a process (rather than a static equilibrium), associating it with a spectrum of alignment ranging from "hard" treaty-based alliances to "soft" alignments (Selden 2013), while also acknowledging many possible types of balancing (Snyder 1991). Indeed, Walt himself recognizes that "balancing is not an instantaneous or automatic process" (Walt 1992, p. 449), without, however, elaborating on the process through which states counteract threats—in other words, how states establish diverse alliances to manage the challenges they face (He and Feng 2012).

In this vein, Walt's understanding of balancing against threat may be seen as a progressive trajectory that eventually ends with the Balance of Power in the system. This reasoning allows us to facilitate our understanding of balancing as a gradual process with different intensities and manifestations, which, when analyzed jointly, demonstrate a coordinated balancing behavior. Given that external balancing represents the strategy of seeking allies for the common cause of confronting a shared threat (Abb 2018), or as Waltz (1987, p. 118) describes it, "moves to strengthen and enlarge one's own alliance or to weaken and shrink an opposing one", external balancing is, thus, approached as a gradual strengthening process (Ross 2006). By adapting the framework of balancing intensity by Roy (2005) that accounts for different levels of balancing intensity targeted toward the perceived threat, we distinguish between high, moderate, and low balancing as gradual manifestations. Moreover, given that a "state's balancing strategies are shaped by the level of threat perception regarding a rival" (He 2012, p. 157), the high intensity balancing, associated with a certain and compelling threat, is more openly adversarial, with the political tensions reducing the possibility of cooperation. Conversely, the low intensity balancing, although indicating efforts to coordinate and join forces between the competitors of the threat, does not exclude a potential constructive relationship with the threat in issues of common importance. Indeed, balancing has been acknowledged to take different forms [and measured in a variety of ways including cooperation intensity (Papageorgiou and Vieira 2023; Papageorgiou and Vieira 2021)], with states resorting to tactics beyond military alliances, including military subversion, strategic arms sales, and arms control decisions, as well as sanctions, embargoes, and instances of non-cooperation and institutional constraints (He 2012). Nevertheless, external balancing in the form of alliances constitutes an expectation of mutual support, given that allies support each other "with all sorts of eventualities which

[7] Bandwagoning in its turn refers to alignment with the dominant power, either to appease it or to profit from its victory. Walt, however, argues that external balancing in the form of alliances is more dominant in history and has more analytical validity.

cannot at the moment be foreseen" (Snyder 1997, pp. 356–357) including less critical issues such as to "agree on a common policy of joint action with respect to those interests" (Snyder 1997, pp. 356–357).

Thus, to account for external balancing in ETs, we distinguish among its three expressions: diplomatic and policy coordination among the main competitors of threat, bans and restrictions/export controls to undermine the threat's power, and instances of strategic alignment that excludes the source of the threat aiming to undermine a rival's power.

The first instance of external balancing behavior corresponds to diplomatic coordination forged to achieve a common approach to ET-related issues (Brattberg 2021). These diplomatic initiatives rely on shared rules, protocols, and behaviors conducive to "a coalition of states that coordinate their actions, to implement a goal" (Goldstein 2020, p. 80) under international policy frameworks. Nevertheless, this policy coordination, initiated due to a threatening actor, constitutes the lowest form of balancing behavior and seeks to avoid raising a counter response while also allowing for maintaining "a constructive relationship with the targeted state" (Roy 2005, p. 306).

Second, we consider the decisions to impose bans and export controls on Chinese technology and infrastructure as a proxy for understanding state behavior, as these measures represent a particular thinking that links technological capabilities directly to a country's national security involving legal and regulatory restrictions or sanctions (Luo 2022). Bans and restrictions are considered more offensive tools and constitute attempts to bring allies on board too (Barkin 2020), indicating a regulatory cooperation (Daniel Mügge 2023). Moreover, the imposition of US restrictions and bans along with their spillover effects enhances the country's own alliance network by building up the capacity of its allies and partners (Schmidt 2022). Accordingly, this indication of "allied technological containment" through bans and restrictions against China shows a moderate and gradual external balancing behavior (Lee and Maher 2022).

Over the past year, the US has engaged in an aggressive campaign to convince European partners to ban Chinese suppliers from their 5G network. Bans restrict market access for a specific company, especially a state-owned enterprise or a company affiliated with a country viewed as a threat, aimed at limiting proliferation of a certain technology. Full bans are indicative of a more intense balancing, contrary to the restrictions indicating a lower intensity balancing behavior. Export controls in their turn also vary in their scope and intensity. For example, within the semiconductor industry, the Netherlands has prohibited the sale of state-of-the-art lithography machines to China, yet China retains the ability to purchase earlier versions of these machines (Jiang 2023). Simultaneously, a total ban implies a complete exclusion of China in transactional relationships.

Finally, the third approach corresponds to instances of strategic alignment (that can translate into alliances, strategic partnerships, security communities, and coalitions (Wilkins 2012; Korolev 2020) that exclude the source of the threat, constituting the highest indication of external balancing, with the intensity of balancing reflected in an (institutionalized) arrangement aimed at promoting interoperability and military preparedness in the ET domain (Rim 2023). And while in the strategic or military domain, expressions of strategic alignment traditionally comprise a defense clause (indicative of an alliance), an establishment of a military base or a joint defense command (Korolev 2020), in the ET domain, respective initiatives excluding the threat-state aim to foster cooperation or joint development of ETs as an alternative to the hostile state (Torreblanca and Jorge-Ricart 2022). Reduced costs of forming alliances in the ET domain and the associated flexibility make it easier for states to build further alliances and provide extended deterrence to a balancing coalition (Mehta 2021). Moreover, cooperation and alignment in ETs reinforces already established alliances and partnerships that remain valuable by facilitating operative cooperation, data sharing, join planning, and risk assessments, while also enhancing the legitimacy of international action (Imbrie et al. 2020), and thus extending beyond the mere dialogue, in contrast to the aforementioned diplomatic initiatives (You 2021).

3 China as an ET Threat: Employing Walt's Quadripartite Approach

We now turn to applying the BoT theory to the development of the ETs, by first, assessing China's threat and the associated aggregate power, geographic proximity, offensive capabilities, and aggressive intentions; and second, by exploring how this threat might be balanced.

3.1 Aggregate Power

According to the Center for Strategic and International Studies, China is a near-peer competitor with the US in AI and advanced computing (Lewis 2019). Some authors even consider China to be ahead of the US and at the forefront, globally, in some fields such as quantum computing (Whalen 2019). Following the idea of threat perceptions intertwined with a change in material capabilities, and examining China's "aggregate power" in ETs, we can observe that the country has made significant advances in various areas while still lagging behind the US in overall technological and research performance (Paszak 2019; Brooks and Wohlforth 2016). This is particularly true of semiconductors (Levine 2020).

Nevertheless, the country's growing and expansive relative ET capabilities, advancements, and incremental growth over a short period of time have positioned it as a threat toward the US. This is supported by US officials' accounts of the ETs, who have stated that "in many ways, it is less important whether their technology is 'as good as ours' than whether it is good enough to render our capabilities ineffective" (Carter 2018, p. 5). Former US Secretary of Defense Mark Esper also voiced the widely shared concern: "I think we need to be very concerned about Chinese technology getting into our systems or the systems of our allies" (Macias 2019) (Table 2).

Artificial intelligence is seen as the sector where China's capabilities have enhanced and come to compete with the US. While in 2019, the US was leading in four categories (talent, research, development, and hardware), and China in two (adoption and data), in 2021, China was continuously reducing the gap in important areas and challenging the US lead, while continuously improving the quality of its AI research, and eventually surpassing the EU in AI publications, according to the Centre for Innovation Data report[8] (Castro et al. 2019; Castro and McLaughlin 2021, para.7). In other assessments, such as 2018 Tsinghua University AI Development Report,[9] China seems to have already secured a leading position in AI, ranking first in the total of AI research papers, highly cited AI papers worldwide, AI patents, and AI venture capital investment and second in the number of AI companies, in addition to the largest AI talent pool.

While China still lags behind in the realm of core AI technologies, such as hardware and algorithm development, and also in top-tier talent where it sees a significant gap with the US, this weakness has already been acknowledged and addressed by establishing an AI talent training system under the auspices of China's Ministry of National Education, supported by the "AI Innovation Action Plan for Institutions of Higher Learning" (Imbrie et al. 2020). According to the latest AI Index report of Stanford University's Human-Centered Artificial Intelligence (2023), there has been a significant surge in Chinese AI publications, increasing 2.3-fold since 2015.[10] China dominated the field between 2010 and 2021, accounting for 39.78% of global AI publications, followed by the EU at 15.05% and the US at 10.03%.[11] As stated in a Stanford University Human-Centered Artificial Intelligence report in 2022, China leads in AI publications, surpassing both the US and the EU, with 22% of total publications, and ranks second in private investment in AI technologies. In 2021, China ranked first in AI publications by sector, followed by the US and the EU. Also, China holds nine positions, in the top ten institutions in the world in 2021 ranked by number of AI publications in all fields, while also leading in Natural language processing publications, AI publications in speech recognition and computer vision, as well as in AI journal publications (Stanford University Human-Centered Artificial Intelligence 2022).[12] In addition, China has been actively exporting AI technologies, either under the Digital Silk Road (DSR) project or via direct trade agreements with individual countries (Greitens 2020), such as with Serbia, which maintains close trade and tech relationships with China in more general terms (Le Corre and Vuksanovic 2019). Huawei alone was able to sell AI-based surveillance equipment to 50 countries along with other tech giants like Hikvision, Dahua, and ZTE (Feldstein 2019). As a result, over 60 countries exclusively use Chinese AI surveillance technology, most of which are in Africa and Latin America, while 36 of them have signed onto China's Belt and Road Initiative (Feldstein 2019). Furthermore, China signed an agreement with 71 countries to deploy smart city public

8 https://datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/.

9 https://indianstrategicknowledgeonline.com/web/China_AI_development_report_2018.pdf.

10 Most of these documents were affiliated with the Chinese government, whereas they were mostly corporate affiliated in the US.

11 Stanford University Human-Centered Artificial Intelligence. (2023). *The AI index report 2023–Artificial Intelligence Index*. Stanford University | AI Index. https://aiindex.stanford.edu/report/.

12 https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf.

Table 2 China's aggregate power in ETs *Source*: Authors' compilation

	Artificial intelligence	Internet of Things (IoT)	Big Data	5G technology	Quantum technologies	Semiconductors
Superior to US	AI global publications 2010 to 2021[a]	IoT patents[c]	Generation of zettabytes[ac]	5G technology patents[f]	Announced government investment in quantum technologies[i]	Share of semiconductor manufacturing capacity[k]
	Leading location for AI located output[b]	Number of Internetof Things (IoT) connected devices from 2020 to 2030 (in millions), by region[d]		Worldwide telecom equipment[g]	Patent applications received by patent offices—quantum communication (2010–2022)[ad]	Market share of semiconductor assembly, packaging and testing[l]
				5G contracts around world[h]		Market share of semiconductor wafer fabrication[m]
		Global market share of cellular IoT modules[e]			Top H-Index Scores for quantum technology by country (communication) (2018–2022)[j]	World silicon production and reserves of one thousand metric tons[n]
						Worldwide primary low-purity gallium production[o]
Incremental growth	AI capacity at the international level[p]		Market value growth[ae]		Quantum computing adoption[t]	
	Leading location for AI located output[q]				Gross domestic spending on R&D[u]	
	AI startup deals in China is on a path to parity with the US[r]				Patent applications received by patent offices—quantum computing (2010–2022)[v]	
	Infrastructure, operating environment, research, development[s]				Top H-Index Scores for quantum technology by country (sensing-computing) 2018–2022[w]	
Significantly behind	AI talent[x]		Big Data and business analytics market share[y]			Global market share of semiconductors sales[z]
US/other actors						Memory chip design[aa]

Table 2 (continued)

	Artificial intelligence	Internet of Things (IoT)	Big Data	5G technology	Quantum technologies	Semiconductors
						Market share of semiconductor manufacturing equipment[ab]

[a]https://cat.eto.tech/

[b]Nature Index The race to the top among the world's leaders in artificial intelligence (nature.com)

[c]China to date, is the world's largest processor of IoT patent applications followed by the USA (2023) https://power.nridigital.com/future_power_technology_feb24/iot-patent-applications-power-industry-2021-2023

[d]https://www.statista.com/statistics/1194677/iot-connected-devices-regionally/

[e]https://www.ft.com/content/cd81e231-a8d3-4bc0-820a-13f525a76117

[f]https://www.statista.com/chart/20095/companies-with-most-5g-patent-families-and-patent-families-applications/

[g]https://www.delloro.com/worldwide-telecom-equipment-up-3-percent-in-2022/

[h]https://www.spglobal.com/marketintelligence/en/news-insights/research/5g-tracker-79-markets-worldwide-have-commercial-services

[i]Source: CSIS China Power Project, https://chinapower.csis.org/china-quantum-technology/

[k]https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/united-states-china-semiconductor-standoff-a-supply-chain-under-stress/

[l]https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/united-states-china-semiconductor-standoff-a-supply-chain-under-stress/

[m]https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/united-states-china-semiconductor-standoff-a-supply-chain-under-stress/

[n]https://pubs.usgs.gov/periodicals/mcs2021/mcs2021-silicon.pdf

[o]https://pubs.usgs.gov/periodicals/mcs2021/mcs2021-silicon.pdf: UNITED STATES GEOLOGICAL SURVEY (USGS) https://pubs.usgs.gov/periodicals/mcs2023/mcs2023-gallium.pdf

[p]The Global AI Index—Tortoise (tortoisemedia.com). https://www.tortoisemedia.com/intelligence/global-ai/

[q]The race to the top among the world's leaders in artificial intelligence (nature.com) link is https://www.nature.com/articles/d41586-020-03409-8

[r]Preqin Note: 2023 data up to June 14 as found on https://www.bloomberg.com/news/newsletters/2023-06-28/artificiai-intelligence-is-the-new-front-line-in-us-china-competition

[s]https://www.tortoisemedia.com/intelligence/global-ai/#data

[t]Organizations in the early or more advanced stages of adopting quantum computing (STATISTA) https://www.statista.com/statistics/1286920/quantum-adoption-by-country/

[u]Source: CSIS China Power Project, https://chinapower.csis.org/china-quantum-technology/

Table 2 (continued)

[v]Source: CSIS China Power Project, https://chinapower.csis.org/china-quantum-technology/

[w]Source: CSIS China Power Project, https://chinapower.csis.org/china-quantum-technology/

[x]The Global AI Index—Tortoise (tortoisemedia.com). https://www.tortoisemedia.com/intelligence/global-ai/

[y]https://www.statista.com/statistics/1258046/worldwide-big-data-business-analytics-market-share-by-country/

[z]2021 Global Market Share State of the US Semiconductor Industry. https://www.semiconductors.org/wp-content/uploads/2022/11/SIA_State-of-Industry-Report_Nov-2022.pdf

[aa]https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/united-states-china-semiconductor-standoff-a-supply-chain-under-stress/

[ab]https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/united-states-china-semiconductor-standoff-a-supply-chain-under-stress/

[ac]China Overtook the U.S. and Will Hold the Largest Share of World's Data at Least by 2025 (yahoo.com) https://finance.yahoo.com/news/china-overtook-u-hold-largest-share-worlds-data-220000709.html

[ad]QED-C | Quantum patent trends update: 2022 | QED-C (https://quantumconsortium.org)

[ae]China: growth rate of big data industry | Statista LINK https://www.statista.com/statistics/1284407/china-growth-rate-of-big-data-industry/ AND DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION COMMITTEE ON DIGITAL ECONOMY POLICY Measuring the value of data and data flows OECD. LINK https://one.oecd.org/document/DSTI/CDEP/GD(2022)1/FINAL/en/pdf

security projects and 447 research partnerships and 145 R&D labs in different parts of the world (Cave et al. 2019).[13]

In terms of Big Data, China's market value was around US$9 billion in 2021, marking a compounded annual growth rate (CAGR) of 31.72% since 2014 (Statista 2021). In comparison, the US market stood at US$21 billion. However, according to forecasts, China is projected to reach a market size of US$42.4 billion by the year 2027 (Businesswire 2020). Close examination of the growth rate of the Big Data industry in China reveals a consistent increase from 2018 to 2021. For instance, while the growth rate was pegged at 18% in 2020, recent estimates suggest that the Big Data industry saw a 30% growth in 2021 (Slotta 2023). This growth is not solely attributed to the sheer volume of data produced, with estimates predicting China will generate approximately 48.6 trillion gigabytes annually by 2025, supported by more than 1 billion internet users. In addition, China generated the most zettabytes of data.[14] These developments constitute deliberate efforts put forth by the CCP since the mid-2010s to exploit data as the fundamental resource of the future global economy and governance system (Liu 2021; Thomala 2023). This concerted effort reached its apex with the unveiling of the comprehensive "Action Plan on Promoting Big Data Development" in 2015 (Gorman 2021). The primary aim of the Action Plan was to leverage Big Data by incorporating it into various sectors such as healthcare (through the extraction of individual health data), transportation, manufacturing, geographical data, and public security (The State Council of the People's Republic of China 2015).

China also plays a significant role in shaping the Internet of Things (IoT), which is growing with the technological footprint of Chinese firms as leading participants in both the development of IoT applications and of the internet's underlying infrastructure; China accounts for three quarters of cellular IoT connections worldwide[15] with three Chinese manufacturers holding over 50% of the global market share of cellular IoT modules.[16]

In addition to this, Chinese manufacturers Huawei and ZTE have become dominant in IoT, selling Radio Access Network (RAN) equipment that forms a critical component of the 5G network. Huawei is leading the global implementation of 5G networks by the number of commercial contracts it has secured, accounting for 91, many of which have been signed with the governments of developing countries in Asia (Bicheno 2020). As Goldman (2020)[17] puts it, Huawei has been dominating "this field with a 30% market share (in 2018)", displaying a growth trend.

[13] Most countries in which China has increased its presence by developing ETs are located in Asia and Africa. China's technology has been employed by repressive regimes to uphold their power, by quelling protests and monitoring political opponents (Feldstein 2019; Greitens 2020).

[14] https://www.cnbc.com/2019/02/14/china-will-create-more-data-than-the-us-by-2025-idc-report.html.

[15] https://merics.org/en/report/connection-everything-china-and-internet-things.

[16] https://www.ft.com/content/cd81e231-a8d3-4bc0-820a-13f525a76117.

[17] As cited in Stautz, S. (2020). China's 5G challenge to the U.S. is for the future—Foreign Policy Research Institute. Foreign Policy Research Institute. https://www.fpri.org/article/2020/11/chinas-5g-challenge-to-the-us-is-for-the-future/.

Like other ETs, quantum technology has become a hotbed of US–China competition. A full materialization of quantum technology can make our current understanding of secure networks and encryption outdated, while revolutionizing the fields of computation, communication, and encryption. The global market value of quantum computing might reach US$1 trillion by 2035 (Howell 2023). Therefore, the prospect of such transformational power further heightens the stakes in this technological race. In recent years, China has stepped up its pace of quantum research through various projects (Smith-Goodson 2019), but its commitment to advancing quantum research is not a recent development. For instance, from 2006 to 2010, a multitude of projects on quantum information was initiated under the auspices of the Ministry of Science and Technology (MOST). This momentum continued into the subsequent "Five-Year Plan", during which China significantly increased its funding support from US$150 million to US$490 million (Zhang et al. 2019). Of particular note, in its 14th 5-year plan (2021–2025), China expressly incorporated quantum technology goals, stating: "We will research and develop intra-city, intercity and free-space quantum communication technologies, develop a general quantum computing prototype and a practical quantum simulator, and make breakthroughs in quantum precision measurement technology" (Center for Security and Emerging Technologies 2021, p. 12). This indicates a clear and strategic intention to emerge as a frontrunner in the field of quantum technology.[18] As it stands, China currently ranks third among nations leading the charge in quantum computing adoption, trailing only slightly behind the US, which is in the first position (STATISTA 2021). However, it is important to remember that quantum computing is still an emerging technology, and its geopolitical implications are subject to unexpected advancements and setbacks.

In terms of semiconductor manufacturing capacity, China surpassed the US in 2020, with a 15% share of the global market compared to the US' 10% (Mark and Roberts 2023). Projections suggest that this gap will widen if current trends continue, with China's share expected to reach 25% by 2030 and the US's share falling to 10% (ibid). The same trend is observed in the world share of semiconductor assembly, packaging, and testing, with China holding a 38% share compared to the US's 5% (ibid). This suggests that China is becoming increasingly dominant in the semiconductor industry, particularly in the manufacturing and assembly stages, something that has sparked US concern and prompted President Biden to issue "Executive Order 14,017 on America's Supply Chains", which establishes semiconductor manufacturing and advanced-packaging supply chains as a priority in the guidelines for sectors posing risks to national security.[19] However, China's reliance on foreign technology and knowledge is evident in the fact that the country has a smaller market share than the US in semiconductor production equipment, memory chip designs, and sales while being the world's largest semiconductor industry.

[18] US' pursuit of quantum supremacy is, however, not a recent endeavor: the US National Science and Technology Council announced the Federal Vision for Quantum Information Science in 2009, followed by National Quantum Initiative Action Plan and the National Quantum Initiative later (Raymer and Monroe 2019), in addition to the quantum information research and quantum chips development (including Google's 53-qubit"Sycamore" undertaken by Google, IBM and Microsoft (Lichfield 2020).

[19] https://www.whitehouse.gov/wp-content/uploads/2022/02/Capstone-Report-Biden.pdf.

The analysis of the dimensions of China's progress in technological development above correlates with the data of both the Global Innovation Index and Development's Frontier Technologies Readiness Index (2023). For instance, as per the Global Innovation Index (2022), China achieved a ranking of 11 in 2022, a notable improvement from its position at 35 in 2013. This advancement is also reflected in the United Nations Conference on Trade and Development's Frontier Technologies Readiness Index (2023), where China ascended to the 9th position among 166 countries, an upgrade from its 15th position in 2021. More strikingly, as per the same index, China surpasses the US in specific categories such as in industry and information communication technologies (ICT), with rankings of 2nd and 9th, respectively, compared to the US's 16th and 11th ranks.

3.2 Geographic Proximity

Geography and distance are key factors in determining plans and strategy, as well as broader security and diplomatic policies of states (Heginbotham et al. 2015). Furthermore, the BoT theory suggests that rising powers like China, geographical proximity "will inevitably induce fear and apprehension among surrounding smaller states" (Chu et al. 2015, p. 406).

Nonetheless, the concept becomes obsolete in the face of the ETs that transcend borders, with threat perceptions no longer confined to surrounding or neighboring states. China's pursuit of global digital leadership in multiple areas, such as digital infrastructure, e-commerce, and research collaboration (Shi-Kupfer and Ohlberg 2019), has been evident in the development of a global Chinese technology network through state-backed companies. Chinese companies supply AI surveillance technology to 63 countries that use exclusively Chinese technology, most of which are in Africa and Latin America (Feldsten 2019). At the same time, state-backed companies such as Huawei, Alibaba, and Tencent have already established their presence in numerous states' telecommunications networks, data centers, and online payment systems. Through initiatives like the Digital Silk Road (DSR), these companies, including Huawei, ZTE, Hikvision, NucTech, and others, are exporting AI technologies, providing support, and directly participating in the deployment and development of various technologies such as cloud computing, smart cities, digital payment systems, and AI within host countries (Greene and Triolo 2020; Feldstein 2019). As this intricate web of digital market interconnections continues to expand, it presents a substantial challenge to other powers irrespective of their geographical locations (Shi-Kupfer and Ohlberg 2019). As such, Beijing's investments in several countries allow China to leverage its global technology power image (Fannin 2020).

For the BoT and the realist paradigm in general, the competition of states for territory, resources and access to important geographical positions is imperative for the power distribution in the international system; as such, the geographic expansion of Chinese manufacturers and suppliers could lead to a significant advantage over other competitors, particularly given Beijing's principle of non-interference in a country's internal affairs when doing business (Papageorgiou 2023). The acquisition of Western firms by Chinese multinationals has increased dramatically in recent years following the Going Global Strategy. Chinese MNEs have used outwards foreign direct investments (OFDI) to acquire brands, advanced technologies, sophisticated management, and marketing skills in developed countries through aggressive strategic asset-seeking M&As (Anderson et al. 2015). For instance, two Chinese companies affiliated with the People's Liberation Army bought three Swedish semiconductor startups in 2018 and bought off British chipmaker "Imagination" and German robot-maker "Kuka" (Braw 2020). These cross-border mergers and acquisitions have raised national security concerns for governments (Williamson and Raman 2011) and have been described as a threat to a hosts' national security (Yang and Deng 2017; Li et al. 2017).

In the semiconductor industry in particular, with its unbalanced global value chain geography privileging a few states, China sought to increase geopolitical space amid the technological race with the US, especially since the latter seeks to return the global center of gravity for integrated circuits (IC) from East Asia back to the US through the "reshoring" of several key industries (Yeung 2022; Triolo 2023).[20]

In addition, ETs such as AI are key to the control of geographic space and the five dimensions (land, sea, air, space, and cyber) of warfare and their interoperability (Fricke 2020). The US and its allies have long benefited from the geography of the internet and its global reach with the most valuable American tech companies gaining the bulk of their revenue outside the United States (Imbrie et at. 2020). Nevertheless, China is on track to possess as much as 30 percent of the world's data by 2030[21] while its Datasphere is expected to be the largest of all regions by 2025 (compared to EMEA, APJxC, U.S.) which will allow it to deploy video surveillance in different parts of the world (Rydning et al. 2018). In addition, given that AI systems know no geographical constraints and are not confined to one geographic region (Lorenzo et al. 2021), "AI-powered intelligence systems may provide the ability to integrate and sort through large troves of data from different sources and geographic locations to identify patterns and highlight useful information, significantly improving intelligence analysis" (Allen and Chan 2017, p. 47), thus expanding the country's global reach but also raising threat perceptions, given that the threat is not only transboundary but can be initiated from anywhere, mitigating the importance of the geographic dimension.

3.3 Offensive Capabilities

This element is particularly important to emerging powers since the offensive capabilities can be used in arms forces. The use of AI, robotics, directed energy, cyber warfare, and orbital systems secure competitive advantages and strengthen deterrence by curbing lower level challenges and achieving strategic advantage. China has developed several systems that could penetrate US defenses. According to some

[20] See also https://www.csis.org/analysis/can-semiconductor-reshoring-prime-us-manufacturing-renaissance.

[21] "The New Racetrack for Artificial Intelligence: China–U.S. competition" [人工智能新赛场 -中美对比], CCID, May 2017.

accounts, "China has likely surpassed the US in the development of a new class of weapons, hypersonic strike vehicles, and may be within months of deploying such systems" (Lewis 2019, p. 6). In addition, the focus is not on military expenditure or the number of military equipment but on the ability to significantly disrupt, degrade, and dismantle military infrastructure.

One could reasonably argue that China's development and enhancement of offensive capabilities position it as a potential threat, even though its defense budget does not align with that of the US.[22] Nevertheless, Xi Jinping has pushed, as indicated in the "Military Strategic Directive for a New Era",[23] for intensifying innovation in ETs to "build a strong military" and reach greater strategic autonomy, while the 14th 5-year plan (2021–25)[24] describes a goal of developing disruptive technologies that would give China a military advantage over rivals and close the gap with the US (Duchâtel 2023).

Concerns related to Chinese technology development have reached an apex when it comes to China's civil–military fusion (CMF) strategy, with US decision-makers constantly referring to the CMF strategy as a malign agenda and a global security threat (Manuel and Hicks 2020). For example, in 2019, then-Secretary of State Mike Pompeo (US department of State, para. 1) stated: "I have been sounding alarm bells to the United States' partners and allies, U.S. corporations, and to the American public about Beijing's strategy of 'Military-Civil Fusion', or MCF [(…)] one of the United States' most pressing national security threats."

At the same time, China's access to European dual-use technology has raised concerns not just for Europe's bilateral relations with China, but also for the management of Europe's relationship with the United States (Duchâtel 2023).

The European Commission's outlining the "European Economic Security Strategy" has emphasized the need "to prevent the leakage of sensitive emerging technologies, as well as other dual-use items, to destinations of concern that operate civil–military fusion strategies" (European Commission 2023). The reason for mounting concerns stems from the blurred nature of China's CMF strategy, which in fact builds upon decades of civil–military integration efforts of previous Chinese leaders (Kania and Laskai 2021). For other states, China's CMF enhances its military capabilities, which could suddenly disrupt the global military balance.

AI also augments cyber capabilities to develop AI-enhanced cyber weapons (or "adversarial AI") which may appear relatively benign, for example, enumerating the target space or repackaging malware to avoid detection and can have significant destabilizing effects in the target countries (Johnson and Krabill 2020). Another area of concern has been China enhancing its military capability by employing "intelligentized warfare" doctrine with the help of AI and ramping up its collaboration with major tech companies such as Hikvision and iFlytek that create two-way around innovation ecosystems (Kania 2017). Moreover, some scholars posit that China may

[22] As per Chinese sources, their defense budget stood at US$230 billion in 2022, reflecting a consistent annual growth rate of 10% from 2000 to 2016 (Heath 2023).

[23] China Daily. http://www.chinadaily.com.cn/specials/whitepaperonnationaldefenseinnewera.pdf.

[24] https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm#C4.

employ ET, particularly AI, in psychological warfare operations to gain decision-making advantages and to anticipate the decisions of enemy forces in the gray zone. Given, also, the Chinese military's growing emphasis on data—that is, the current informatization (information-driven) and future intelligentization (artificial intelligence-driven) views of warfare—one can conclude that the ability to manipulate information, broadly defined as information warfare (信息战),[25] including the ability to manipulate how adversaries receive and process that information (psychological warfare) has become one of China's foremost priorities (Beacuchamp-Mustafaga 2023).

Lastly, regarding the prospective development of lethal autonomous weapon systems (LAWS), despite having repeatedly supported a legal ban on LAWS, China has been promoting a narrow understanding of these systems that intends to exclude such systems from what it deems "beneficial" uses of AI (Qiao-Franco and Bode 2023). In addition, the fact that the People's Liberation Army (PLA) is using MCF to "weaponize biotech" using CRISPR gene-editing technology, advanced biomimetic systems, biological and biomimetic materials and human performance enhancement (Kania and VornDick 2019) indicates the offensive nature of the country's capabilities. Considering the potentially transformative impacts of ETs across various military strategic domains, and recognizing the role of AI as a force multiplier, it becomes apparent that if an adversary's AI systems lack attributes such as transparency, reliability, and verifiability, it becomes challenging to accurately gauge the adversary's capabilities (Johnson 2020). Thus, it becomes harder to objectively assess their deterrent threat credibility, while concerns grow about how these technologies can bolster a state's offensive capabilities and heighten other states' threat perceptions.

3.4 Aggressive Intentions

The US government has repeatedly raised its concerns regarding potential security risks from these companies due to the influence of the Chinese government over its firms, proclaiming that the Chinese government "may force Chinese suppliers or manufacturers to modify products to perform below expectations or fail, facilitate state or corporate espionage, or otherwise compromise the confidentiality, integrity, or availability of IoT devices" (USCC, 2018, p.461). Given China's notorious cyber-attacks reputation, new tensions pertaining to the AI-cyber nexus may emerge in the near future. Cyber tactics such as cyber espionage and attacks have become a cost-effective modus operandi for states, especially China, in relation to ETs and offer a means to acquire otherwise inaccessible or heavily guarded information, providing a substantial advantage in the rapid advancement of these technologies. According to US think tank, the Center for Strategic and International Studies, between 2000 and 2023, 224 incidents were recorded, with 49% involving actors tied to the Chinese military and government. Moreover, over 1200 cyber espionage cases in

[25] More on modern Chinese operational concepts, see (Burke et al. 2020).

either China or the US are currently under investigation (CSIS 2023a, b). Some estimates propose that the US economy suffers an annual loss of US$300 billion due to Chinese cyber espionage operations, affecting areas from quantum computing and semiconductors to AI (Laskai and Segal 2018). Over time, there have been longstanding allegations of cyber espionage efforts by China along with forced technology transfers through mergers with Western companies, which have raised significant concerns among the US and its allies and partners (Lindsay et al. 2015). At the same time, in its 2022 Annual Threat Assessment, the Office of the Director of National Intelligence (ODNI) included the following passages regarding China's cyber capabilities and intentions: "China presents the broadest, most active, and persistent cyber espionage threat to US Government and private sector networks. China's cyber pursuits and export of related technologies increase the threats of attacks against the US homeland. China almost certainly is capable of launching cyberattacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems" (ODNI 2022, 8). Between 2005 and 2022, 237 cyber operations carried out by China (state sponsored) were reported (according to Council of Foreign Affairs Cyber Operations Tracker 2023), which can be interpreted as aggressive actions of malicious intent.

Similarly, China's disinformation campaigns reinforce the assessment of China's intentions as aggressive. Since 2015, has expanded social media disinformation campaigns, and established a separate unit for the conduct of information warfare, the PLA Strategic Support Force (PLASSF) (Harold et al. 2021). While China has been mainly using information manipulation domestically, for instance, during the Hong Kong protests using Western social media such as Twitter (Beskow and Carley 2020), its latest extensive disinformation campaigns have posed a significant risk to US and other actors' intelligence operations and national security. Indeed, China (similar to Russia) has been accused of spreading disinformation campaigns and propaganda amid the COVID-19 crisis by both the EU and the US (European Parliament 2020; US Embassy in Georgia 2020), with the goal of advancing "anti-Western views, and spread[ing] false information to create divisions between the United States and its partners and allies" (White House 2020, p. 7).

Finally, when it comes to intellectual theft, the US has accused Chinese companies of stealing or misusing intellectual property rights from US companies and also forced technology transfers (van der Linden and Łasak 2023). For instance, the 2021 Microsoft Exchange breach, linked to APT31 and APT40, compromised 300,000 organizations globally as claimed by Microsoft, the United Kingdom (UK) and other countries (Jarnecki and Dawda 2023). Accordingly, in their newly initiated national cyber strategies, countries like the US and the UK, have characterized China as a "systemic competitor"[26] and indicated that its aggressive acts in cyberspace pose national challenges while also indicating that "states with revisionist intent are aggressively using advanced cyber capabilities to pursue objectives that

[26] UK government. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022.

run counter to our interests and broadly accepted international norms".[27] China's global position, particularly in the realm of ETs, can be, thus, characterized as assertive or aggressive in our framework of analysis.

4 External Balancing Against China in the Realm of ET

The external balancing strategy in ET aims to achieve two primary goals: first, to outspend China and restrict its access to certain critical technologies, new markets,[28] and resources required for its technological progress and to counter Chinese technology acquisition, and second,[29] to stablish a network of allied states to coordinate such initiatives.[30]

4.1 Diplomatic and Policy Coordination

The first approach indicates that external balancing behavior is diplomatic coordination of policy responses with the threat's main rivals in either a bilateral or multilateral form. Indeed, the primary aim for the US is to safeguard its technological dominance by rallying other countries around itself while simultaneously curbing China's technological expansion, especially in nations participating in the Digital Silk Road initiatives. In September 2021, the US and the EU issued the TTC Inaugural Joint Statement, announcing cooperation on export controls that go beyond traditional objectives, to combat human rights abuses as well as address concerns about ETs, signifying a potential alliance to counter Chinese technology expansion (Chorzempa and von Daniels 2023). The European Commission, in its turn, proposed an EU–US Trade and Technology Council to strengthen joint technological leadership, leading in future to an increase in multilateral PPPs as well as international cooperation regarding R&D, standards-setting and good governance practices regarding the application of technologies (Capri 2020). At the same time, it shows that the EU's active engagement and interest in international collaboration around AI is matched with positive perceptions of the US' role as an AI partner (Cohen and Fontaine 2020).

In a similar vein, to coordinate joint initiatives, the State Department elevated the Clean Network initiative[31] to an international collaboration network aimed at restricting Chinese tech expansion, particularly in developing countries, such as on the African continent. The announcement of this initiative composed by countries,

---

[27] US government, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[28] ODNI (Office of the Director of National Intelligence). 2022. "Annual Threat Assessment of the US Intelligence Community." February. www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2279-2022-annual-threat-assessment-of-the-u-s-intell igence-community.

[29] Council of foreign Affairs Cyber operations tracker https://www.cfr.org/cyber-operations/.

[30] An example is the 2014 breach of the US Office of Personnel Management (OPM), which led to the theft of sensitive information of over 22 million individuals. See (Mohamed et al. 2018).

[31] See The Clean Network. (2020). U.S. Department of State. https://www.state.gov/the-clean-network/.

telecom companies and suppliers, despite its limited impact, was characterized as an "effective way to call attention to the problem of Chinese technological espionage" (Kuo 2021, par. 2) and to urge US allies and partners to avoid Huawei and other Chinese ICT firms from their 5G networks, opting for their competitors such as Ericsson and NOKIA.

In the same context, in 2019 and 2020, the US State Department initiated a series of "Joint Declarations on 5G Security" with allies in Eastern and Central Europe (except Hungary) to raise awareness of countries who are keen on adapting Chinese 5G networks. Furthermore, in the western Balkans, North Macedonia signed a similar declaration, Kosovo signed a Memorandum of Understanding, and Albania stated its intention to join the Clean Network initiative in 2020 (Taylor 2022; US Department of State 2020; Friis and Lysne 2021). Lastly, most recent diplomatic initiatives, such as the one in July 2022 between the US and Japan, include the formation of a high-level dialogue focused on semiconductor cooperation to counter China's growing economic influence (CSIS 2023a, b).

One of the most prominent examples of joint initiatives between states threatened by China that aim to support China's key rivals is the US allowing Taiwanese semiconductor companies to set up a factory on US soil in Arizona (Disis 2020; Swanson et al. 2020). Given that TSMC holds around 90 percent of the market share for advanced processors used in most of the world's electronic devices, as well as in more advanced technologies such as guided missiles and machine learning (ML) applications, the decision to build a second factory in Phoenix[32] despite no significant economic benefits for TSMC or Taiwan further indicates that this decision was facilitated by political considerations and most specifically the geopolitics of chip production, driven partly by fears over China's hostile posture toward Taiwan (Liu and Mozur 2023[33]); this indicates that states perceiving China as a threat seek to join forces. Moreover, the dramatic acceleration in the US effort to control the rise of China's advanced semiconductor sector and its attempts to engage with partners and allies to achieve that end, and the fact that TSMC also severed ties with Huawaei in May 2020, shows the increasing difficulty companies and countries face to remain insulated from geopolitics (Mark and Roberts 2023).

Initiatives akin to these have also been pursued with South Korea, evident in Samsung's monumental US$17 billion investment project in Texas, and with Japan across various ETs, including semiconductors (Hotta 2022). On an interesting note, European countries have also adopted similar initiatives, such as Germany's recent signing of an agreement to build a US$11 billion chip manufacturing plant in the country.[34]

32 https://www.ft.com/content/d0fe3dda-7ea4-4d37-9564-71a129b9002f.

33 https://www.nytimes.com/2023/02/22/technology/tsmc-arizona-factory-tensions.html.

34 https://www.scmp.com/news/china/article/3230440/tsmc-build-us11-billion-chip-manufacturing-plant-germany.

4.2 Bans and Restrictions

Export controls and bans have played an increasingly important role in the US government's efforts to deny China access to critical technologies (Fischer 2023). As such, the referred measures initiated by the US aim to slow Beijing's advances in ETs. By imposing export sanctions, the US is trying to force technological decoupling and disable the functioning of global supply chains in the domains critical for Chinese high-tech to slow down or contain China's technological and economic rise (Milutinovic and Nikolic 2023). Accordingly, the US has called its allies to protect their shared democratic values in the technological sector, ascribing even an ideological connotation to its response to Chinese tech expansionism and emphasizing its fear of digital authoritarianism diffusion (Shahbaz 2018). As the US cannot address these challenges in isolation, collaboration among its treaty allies becomes imperative, involving the sharing of sensitive advanced technologies with national security and military applications and civil and military technology research and (co-)development, (co-)production, and joint ventures, in addition to flexible partnerships with non-traditional-US allies (Limaye and Tenyotkin 2023). For example, the coordinating group has shaped a common approach on export restrictions in the semiconductor manufacturing equipment sector, in which the coordination with Japan and the Netherlands possessing advanced photolithography technologies proved essential. It has laid out a position on whether to allow US chipmakers to continue selling commodity chips to Huawei while restricting the export of the most advanced semiconductors and chip fabrication equipment (Lewis 2020).

At the same time, as the US has pressured its allies to adopt export controls and bans, the varied response of different states indicates a gradual intensity of balancing behavior, with a full ban corresponding to the "full rejection of Huawei (in accordance with US preference)" (Christie et al. 2023, p. 8), considered here a stronger expression of balancing efforts, distinct from other restrictions. The latter, which share a commonality with bans of states' being markedly more acceptive of US policies/recommendations, include laws posing substantial barriers for Huawei, or 5G security agreements with the US, as well as 5G contracts concluded by state's telecom operators with Huawei competitors (Nokia, Ericsson, local actors) (Christie et al. 2023), and are indications of balancing of lesser intensity. Therefore, both behaviors further confirm the BoT theory that threat perceptions of China lead to external balancing.

Regarding bans, during Donald Trump's presidency, concerns escalated over how Chinese companies were using data, with ongoing debates about the degree to which Chinese big tech firms were participating in military projects (Kokas 2022; Mishra et al. 2022). In May 2019, Trump issued an executive order (extended in May 2020) laying the groundwork for a ban on Huawei equipment in US networks from using telecommunications equipment or cooperating with critical software and licenses (such as Huawei, ZTE).[35] This move expanded the restrictions enacted in 2018

[35] See https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

regarding the use of Huawei by US agencies and federal contractors. In June 2020, the FCC formally designated Huawei and its affiliates (along with ZTE) as posing such a threat. The Trump administration initially urged, and then even pressured, US allies to ban Huawei from providing 5G network infrastructure (Gray 2021).

The US has been actively pressuring Huawei to limit its market access and involvement in 5G network development worldwide, citing concerns that the Chinese Communist Party could exploit the company for espionage, compromising other nations' critical infrastructure and granting China significant influence over global telecommunications networks (Christie et al. 2023). The promotion of a comprehensive 5G technical dossier has become a matter of a distinct choice between competing alliances spearheaded by the US and China (Calcara 2023). A great deal of countries sided with the US, with the UK enacting an outright ban of Huawei from the rollout of 5G infrastructure by 2027 removing equipment from earlier generations (Kahata 2020), eventually admitting "geopolitical" concerns behind the ban (Leoni 2022). They were followed by Japan, Sweden, and New Zealand with their behavior corresponding to external strategic balancing (Cheung and Wilhelm 2020; Yasir and Kumar 2020). Despite earlier more sceptical approaches to the outright ban of Huawei, European states decided to enact legal actions (Kahata 2020) to restrict access and moved toward bans. This is the case of the Italian government's veto of the 5G deal between Huawei and Italy's telecom company FastWeb (Kahata 2020), whereas other European states (including Denmark, France, and more recently, Germany) have imposed significant restrictions, alongside Israel and India (Christie et al. 2023). While balancing efforts are typically associated with more advanced, industrialized countries, the US and its European allies have exerted pressure on other nations to join in countering China's Huawei; this pressure has been applied to countries such as Kenya, Costa Rica, the Philippines and Jamaica, (Pollet and Handel 2023). Another example has been Ethiopia's 5G network auction in May 2021 which saw Vodafone, backed by the USIDFC, outbid the Huawei-supported MTN, displaying balancing of an African country against China's ICT influence (Woo and Wexler 2021).

In addition, the US has adopted the same approach to counter China's influence in the semiconductor sector, as evidenced by the executive order in June 2021 to address the "threat posed by [China's] military-industrial complex" (White House 2021a, b), forbidding investments in 59 Chinese companies, including Huawei and Semiconductor Manufacturing International Corporation (SMIC) and the enactment of the CHIPS and Science Act in 2022 (White House 2022b). This legislation aims to bolster the domestic semiconductor industry through significant capital investment, amounting to US$280 billion (Badlam et al. 2022). It includes provisions for US$39 billion in subsidies to support onshore chip manufacturing and offers a 25% investment tax credit for expenditures related to manufacturing equipment. In conjunction with these efforts, US citizens and green card holders are prohibited from working on certain chip technologies for Chinese entities, further reinforcing the strategy of restricting China's access to advanced technology (Badlam et al. 2022). Other countries have followed in the US' footsteps, such as Japan, the Netherlands, Germany, and even the EU as a whole have also implemented restrictions on Chinese semiconductor exports. As such, in January 2023, the US reached an agreement with both the Netherlands and Japan to deny some advanced chip manufacturing machines to China and to restrict sales of equipment for advanced semiconductors to China (Edwards 2023). The acceptance of US policy recommendations, which sometimes takes place following months of arduous negotiations, embodies a united effort from the US and its allies to impede China's acquisition of state-of-the-art semiconductor technology with the objective of preserving their own technological superiority (Sheehan 2022; Ting-Fang et al. 2023).

Moreover, real-life applications of ETs such as TikTok and WeChat have been used as a pressure mechanism on US allies. The US has labeled TikTok as a potential risk to national security, attributing concerns to its perceived close ties with the Chinese government and the presence of party officials in significant positions within the company (Johnson 2023). Thus, the approval of the "No TikTok on Government Devices Act" and two consequential acts, namely the DATA Act and the RESTRICT Act, were introduced to the US Congress with the aim of further limiting third-party usage of private data (Bordelon 2023). As of 2023, the use of TikTok on government-issued devices has been prohibited for state government agencies, employees, and contractors in 34 out of 50 US states (Richmond 2023). Similarly, several other countries (see list in AP News 2023) have again adopted foreign policy recommendations, including Jordan and Taiwan, along with the EU, Belgium, Canada, Ireland, Norway, and the UK (all of which have enacted restrictions on the use of certain devices by government entities and staff) (Iyengar 2023). India, on the other hand, banned both TikTok and WeChat completely in 2020 and restricted the participation of ZTE and Huawei in 5G network infrastructure building (Zaveri 2023).

Overall, the US has managed to convince its allies from Western Europe to East Asia to cease exporting "sensitive technologies" in sectors such as AI and microprocessor manufacture, and, to borrow the wording, Qiu (2023), a single dominant billiard ball (the US) has led numerous other billiard balls (US allies) to set their policies accordingly, including the pressure to prevent the selling of EUV lithography equipment to China (mainly Netherlands) in the framework of the Wassenaar Agreement.

4.3 Strategic Alignment: Alliances and Strategic Partnerships

The third expression of external balancing in ETs is strategic alignment in the form of semi-formal alliances and strategic partnerships, which allow for joint efforts, sharing of information, and technology cooperation (Han and Paul 2020). At the same time, this strategic alignment in most cases is already embedded in a broader security framework and draws more commitments of expressions of mutual support by allied members. All these developments are efforts by the US and its allies to achieve mutual support on the issues that are below their alliance contract (Lee et al. 2022). In line with BoT theory, when states recognize another state as a threat, they form balancing coalitions to counter the threat; in ETs, the US has turned to its allies and partners to counter Chinese clout in global technology (Lee et al. 2022). Semiconductors and AI in particular have been identified as the key technologies for successful external balancing strategies, with the US promoting an alliance-centered reorganization of semiconductor supply chains (Lee 2023; Grochmalski et al. 2020). Washington's focus on semiconductors is due to their enabling nature, as well as because China has so far failed to catch up with market leaders in critical industry segments. The Biden administration aims then to persuade allies to endorse US policy toward China without alienating them by applying too much pressure in an attempt to motivate allied governments (Fisher 2023). The US has even called for "friend-shoring" in semiconductors to bring the production back to the US and its like-minded allies (Coy 2021). The Biden administration has not only expanded upon the direct economic engagement with China initiated by the Trump administration (structural power of exclusion), but it has also sought to strengthen its international network of alliances (structural power of influence) (Erlbacher and Schmalz 2023). As such, they have retained most of their foreign economic policies toward China, imposing further sanctions on the semiconductor chip industry (CHIPS Act of 2022) and adopting an interventionist industrial policy approach (Inflation Reduction Act of 2022). The US has also sought to close ranks with its traditional allies in Europe by designing joint initiatives (creation of the US–EU Trade and Technology Council) (Erlbacher and Schmalz 2023). During the Biden administration, the US has pursued a multilateral, ally-focused approach to advance technology agreements through bilateral and multilateral arrangements (You 2021). These include the Chip 4/Fab Four alliance, the Quad, AUKUS, and an extensive collaboration with China's rivals/competitors, such as Taiwan, Japan, and South Korea. The June 2019 AI partnership with Singapore on the development and use of AI technologies in the national security domain was one of the first initiatives of strategic alignment in ETs (Parameswaran 2019). In addition, the US, EU, and Japan have joined forces in conducting joint R&D on ultrafast computers and secure communications, seeking to counter China's rise in quantum computing (Oikawa 2019).

The formation of the Chip Four[36] or Fab Four,[37] a semiconductor supply-chain resilience working group, between the US, Japan, Taiwan, and South Korea has indicated the strategic alignment between US and its close allies in coordinating efforts to restructure global semiconductor supply chains to reduce reliance on China, protect relevant companies' intellectual property (IP) and coordinate export controls (Zhang 2021[38]). This foreign policy initiative by the US and its acceptance by major semiconductor manufacturers, namely South Korea, Japan, and Taiwan, aim at reducing Chinese economic coercion and market distortion (Corrado 2023).

Furthermore, the renewal of the Quadrilateral Security Dialogue (QUAD) between the US, India, Japan, and Australia brings ETs to the forefront, being one of the three collaboration initiatives promoted by the four states (White House 2021a, b). The Quadrilateral Security Dialogue has been working to establish standards

[36] The Chip-4 alliance was proposed by Biden in March 2022 to bring together chip producers South Korea, Japan, Taiwan, and the United States to partner on a semiconductor supply alliance.

[37] https://focustaiwan.tw/business/202302250013.

[38] https://www.gisreportsonline.com/r/us-china-chip-race/.

on AI and bolster the resilience of the semiconductor supply chain.[39] Through the Quad Cybersecurity Partnership, Quad partners cooperate on critical infrastructure protection, supply-chain resilience and security, workforce development and talent, and software security standards (White House 2022a, b).[40] Indeed, the Quad's cybersecurity initiatives are meant to deal with threats from China and bolster cyber resilience, not develop offensive cyber capabilities (Patil 2022). In addition, Quad's discussions on cybersecurity and interoperability focus on adopting a "collective approach to enhancing cybersecurity" through initiatives like Quad Cybersecurity Partnership as guided by the 10 Joint Cyber Principles.[41] At the same time, QUAD's initiatives are organized into three functions; regional public goods provision, mutual resilience enhancement, and standard setting for critical and emerging technologies driven by three major endeavors: balancing, order-building, and management of China as a threat (Satoru 2021). Furthermore, the US–Japan–ROK cooperation in areas like R&D and supply-chain security constitutes also a strong complement to the QUAD mechanism, indicating that the United States and its allies are actively supporting each other in technology and enhancing supply-chain security (Qi 2023).

AUKUS, comprising Australia, the UK, and the US, has also emphasized ETs as a potential countermeasure to the perceived Chinese threat in the region. Beyond their agreement on constructing nuclear-powered submarines, the partnership has launched various initiatives in the realm of ETs. These include the AUKUS Quantum Arrangement (AQuA), trilateral cooperation on AI, the AUKUS Undersea Robotics Autonomous Systems (AuRAS) and advanced cyber initiatives (White House 2022a). Through the focus on ETs, the US is enhancing its balancing act by leveraging its alliance with AUKUS and the Enhanced Force Posture Cooperation launched by AUSMIN (Satoru 2021). In addition, AUKUS' focus on ETs aligns with the global trend of competing for pre-eminence in emerging technologies and its subsequent translation to military dominance (Taylor 2022). Finally, the joint advisory on Cyber Threats[42] released by the Five Eyes alliance in May 2022 highlights a concerning trend: the rise in cyberattacks perpetrated by nation-state threat actors targeting managed service providers (MSPs) (Oxford Analytica 2023). This advisory not only serves as a warning but also demonstrates the alliance's commitment to aiding critical infrastructure network defenders in their efforts to identify and combat these threats. In addition, at the recent 'Emerging Technology and Securing Innovation Security Summit', high-ranking officials from the Five Eyes Countries expressed a profound concern for an unparalleled threat posed by China in high-tech sectors (Financial Times 2023). Indeed, this underscores a deeper level of strategic

[39] White House, "Fact Sheet: Quad Leaders' Summit," September 24, 2021, https://www.whitehouse.gov/briefingroom/statements-releases/2021/09/24/fact sheet-quad-leaders-summit/.

[40] White House (2022a, b). "FACT SHEET: Quad Leaders' Tokyo Summit 2022." May 23. www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/factsheet-quad-leaders-tokyo-summit-2022/.

[41] "Quad Cybersecurity Partnership: Joint Principles", Ministry of Foreign Affairs of Japan. https://www.mofa.go.jp/files/100348060.pdf.

[42] CISA. https://www.documentcloud.org/documents/21985540-cisa-joint-advisory-on-cyber-threats-to-msps?responsive=1&title=1.

alignment within the alliance, extending beyond traditional information sharing, and illustrating their mutual support and coordinated approach in safeguarding their systems and infrastructure. With these initiatives, the US seeks to reinforce cooperation with its key allies to stay ahead of China and counter its technological advances in semiconductors, AI, and Big Data by raising institutional, administrative, and market barriers against competitors in both informal, diplomatic, and formal alliance settings (Malkin and He 2023). The exclusion of the threatening actor from strategic alignments further corroborates instances of balancing behavior (Table 3).

5 Discussion and Conclusion

China's growing power and expansion in ETs are key to driving momentum of the global shifts in technology and the geopolitical landscape. ETs such as AI, quantum computing, the IoT, 5G and Big Data have been transforming the material distribution of power in the global order and challenging traditional theoretical considerations. China and the US have engaged in unprecedented competition in ETs, and the growing use of ETs both in civilian and military domains by China has escalated China's stakes as a threat.

The present contribution has examined how China's ET advancements have resulted in the perception of this country as a threat, through the theoretical lens of the BoT theory. While the multidimensionality and interconnectivity of ETs make geographical proximity an obsolete criterion for threat perception, the other criteria (aggregate power, offense-defense balance, aggressive intentions) hold true in what regards the constitution of threat and the respective state behavior in response to it. China's aggregate power (analyzed by focusing on AI, 5G, Big Data, quantum computing, semiconductors) firmly establishes China as a near-peer competitor to the US (China is even superior to the US in some indicators in each category), displaying rapid and constant growth in its development of ETs. In parallel, China's advancements in civil–military fusion secure a potential strategic advantage by enhancing China's military capabilities. Finally, China's aggressive intentions have been reflected in its covert operations that have grown in number, frequency, and more reach.

The balancing behavior adopted by Western states faced with the growing threat posed by China has found its reflection in various forms, including diplomatic efforts aimed at undermining China's ET power, bans, and restrictions of Chinese companies (as in 5G) and use of social media applications, and securing monopoly over the critically important production of semiconductors. Balancing behavior also includes instances of strategic alignment excluding or targeting China. Thus, one can conclude that, in the context of US–China strategic rivalry, the US has sought to counter Chinese clout in global technology leadership by leveraging its extensive network of allies.

The present analysis allows us to draw three conclusions relative to the dynamically evolving research of ETs. First, by reading into the latest years' developments, we can conclude that ETs will be determinative in the distribution of the Balance of Power, with possible implications for the international system's polarity. However,

Table 3 Manifestations of gradual intensity of external balancing against China in ETs. *Source*: Authors' compilation

Intensity of balancing	External balancing in ET	Examples of external balancing in ET
Low	Diplomatic and policy coordination among competitors of the threat	US–EU TTC, Clean Network, TSMC semiconductors agreements
Moderate	Bans and restrictions to undermine a rival's power	Semiconductors, Huawei, TikTok, WeChat
High	Strategic alignment (alliances, strategic partnerships) excluding/targeting the threat	Quad, AUKUS, Fab Four, Five Eyes Joint Advisory, US–Japan–ROK trilateral cooperation

we can also observe the formation of spheres of influence and increased competition at the early stages. Thus, while clear-cut considerations of alliances might not be as prevalent as in the Cold War period, balancing dynamics are already in place.

Second, the validation of BoT theory in the ET domain contributes to the debate between the Balance of Power and BoT theories, while also proving the relevance of the realist IR paradigm in explaining contemporary phenomena. The BoT offers a more compelling explanation of individual states' behavior in the ET domain when compared to the Balance of Power hypothesis of states' balancing the strongest actor in the system, which is still the US. To be sure, most of the analyzed states are already US allies, and it could be argued that the arrangements in the ET domain or individual decisions such as bans or export controls simply add another layer to the already existing alliance. However, new arrangements that exclude China as well as the diplomatic coordination aimed at undermining China does not always include the US. Instances of cooperation among the analyzed states, such as between Germany and Taiwan's (the world's largest) semiconductor manufacturing company, TSMC confirms the validity of the BoT theory. The present article, therefore, aligns with the contributions that, after putting the BoT to the test in the ET domain, have found that the theory holds considerable explanatory power both in terms of identifying the sources of threat and also in predicting how states will respond to threat.

Third, we concur with contributions arguing that there are different manifestations, intensity, and types of balancing, which, when analyzed jointly, allow for the identification of coordinated balancing behavior, namely, instances of diplomatic coordination among competitors of the threat, bans, and restrictions aimed at undermining the threat's power in the ET domain as well as instances of strategic alignment excluding the threat. The BoT theory's original notion of balancing against threat as a 'response' may be, therefore, presented in a more fine-grained manner if the balancing response is viewed as a process with different steps and stages, even though more academic attention is necessary here, and while it is important to highlight that mutual support is a common denominator bringing together different types of alignment that represent manifestations of the same behavior, external balancing.

The dynamically evolving ETs constitute a key strategic area of competition in IR and call for future research. This concerns especially analyzing state behavior adopted in response to China's ET threat by focusing on more cases of states adopting specific measures and strategies. In addition, the BoT offers a fruitful avenue of future research by distinguishing not only offensive capabilities but also aggressive intentions. The latter can be explored in an especially promising way from non-realist perspectives, particularly the constructivist one, given its special attention to the issue of state interaction, national identity, status and historical experiences. At the same time, the analytical framework of this study and conceptualization of external balancing in ETs can lead to further testing while the opposing argument of bandwagoning with the threatening state could also be explored through the relations of China with other friendly nations, most notably Russia, Pakistan, and North Korea.

Funding Funded by the Research Center in Political Science (UIDB/CPO/00758/2020), University of Minho and supported by the Portuguese Foundation for Science and Technology (FCT) and the Portuguese Ministry of Education and Science through national funds. For the purpose of open access, the author has applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising from this submission' supported by the University of Exeter.

Declarations

Conflict of interest The authors declare that there is no conflict of interest.

References

Abb, P. 2018. What drives interstate balancing? Estimations of domestic and systemic factors. *International Politics* 55: 279–296.

Adams, K.R. 2003. Attack and conquer? International anarchy and the offense-defense-deterrence balance. *International Security* 2003: 45–83.

Alderman, D., and J. Ray. 2017. Best Frenemies forever: Artificial intelligence, emerging technologies, and China–US strategic competition. *SITC Research Briefs* 2017: 1.

Allen, G., and T. Chan. 2017. *Artificial intelligence and national security*. Cambridge, MA: Belfer Center for Science and International Affairs.

Allison, G.T. 2017. Destined for war? *The National Interest* 149: 9–21.

Allison, G., and E. Schmidt. 2020. Is China beating the us to AI supremacy? Harvard Kennedy School. *Belfer Center for Science and International Affairs* 2020: 1.

Anderson, J., D. Sutherland, and S. Severe. 2015. An event study of home and host country patent generation in Chinese MNEs undertaking strategic asset acquisitions in developed markets. *International Business Review* 24 (5): 758–771.

Anwar, N. 2023, February 8. World's largest drone maker is unfazed - even if it's blacklisted by the US.CNBC. https://www.cnbc.com/2023/02/08/worlds-largest-drone-maker-dji-is-unfazed-by-challenges-like-us-blacklist.html#:~:text=DJI%20currently%20dominates%20more%20than,by%20its%20founder%20Frank%20Wang

AP News. 2023. https://apnews.com/article/tiktok-ban-privacy-cybersecurity-bytedance-china-2dce297f0aed056efe53309bbcd44a04.

Australian Strategic Policy Institute. 2023. Mapping China's Tech Giants | ASPI | Australian strategic policy institute. aspi.org.au. https://chinatechmap.aspi.org.au/

Ayoub, K., and K. Payne. 2016. Strategy in the age of artificial intelligence. *Journal of Strategic Studies* 39 (5–6): 793–819.

Badlam, J., Clark, S., Gajendragadkar, S., Kumar, A., Orsquo, Rourke, S. S., and D. Swartz. 2022, October 4. The Chips and Science Act: Here's what's in it. McKinsey & Company. https://www.mckinsey.com/industries/public-sector/our-insights/the-chips-and-science-act-heres-whats-in-it

Bak, D. 2018. Alliance proximity and effectiveness of extended deterrence. *International Interactions* 44 (1): 107–131.

Barkin, N. 2020. Export controls and the US-China tech war. *MERICS China Monitor* 18: 1.

Beauchamp-Mustafaga, N. 2023, June 1. Chinese next-generation psychological warfare. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA853-1.html

Beskow, D. M., & Carley, K. M. 2020. Characterization and comparison of Russian and Chinese disinformation campaigns. Disinformation, misinformation, and fake news in social media: emerging research challenges and opportunities, 63–81.

Bicheno, S. 2020, February 20. Huawei is still the leader on 5G commercial contracts. Telecoms. https://telecoms.com/502562/huawei-is-still-the-leader-on5g-commercialcontracts/
Bordelon, B. 2023, March 31. Congress goes wobbly on TikTok. POLITICO. https://www.politico.com/news/2023/03/31/senate-tiktok-bill-restrict-act-00089926
Brattberg, E. 2021. Middle power diplomacy in an age of US-China tensions. *The Washington Quarterly* 44 (1): 219–238.
Braw, E. 2020. How China Is Buying Up the West's High-Tech Sector. https://foreignpolicy.com/2020/12/03/how-china-is-buying-up-the-wests-high-tech-sector/
Bremmer, I., and C. Kupchan. 2018. Top risks 2018. https://www.eurasiagroup.net/files/upload/Top_Risks_2018_Report.pdf
Brooks, S.G., and W.C. Wohlforth. 2016. The once and future superpower: Why China won't overtake the United States. *Foreign Affairs* 2016: 1.
Browne, R. (2023, June 21). Top EU official urges more countries to ban China's Huawei, ZTE from 5G Networks. CNBC. https://www.cnbc.com/2023/06/16/eu-urges-more-countries-to-ban-chinas-huawei-zte-from-5g-networks.html#:~:text=The%20U.S.%20and%20its%20allies,Beijing%20have%20denied%20the%20allegations.
Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., and D. Amodei. 2018. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Preprint arXiv:1802.07228.
Burke, E. J., Gunness, K. A., Cooper, C. A., & Cozad, M. R. 2020. People's Liberation Army operational concepts (p. 32). Santa Monica, CA: RAND.
Buzan, B. 1991. New patterns of global security in the twenty-first century. *International Affairs* 67 (3): 431–451.
Cai, C., and R. Zhang. 2023. Malicious use of artificial intelligence, uncertainty, and US–China strategic mutual trust. In The Palgrave handbook of malicious use of AI and psychological security, pp. 377–396. Cham: Springer.
Calcara, A. 2023. From quiet to noisy politics: Varieties of European reactions to 5G and Huawei. *Governance* 36 (2): 439–457.
Campion, A.S. 2020. From CNOOC to Huawei: Securitization, the China threat, and critical infrastructure. *Asian Journal of Political Science* 28 (1): 47–66.
Can, M., and H. Kaplan. 2020. Transatlantic partnership on artificial intelligence: Realities, perceptions and future implications. *Global Affairs* 6 (4–5): 537–557.
Can, M., and A. Vieira. 2022. The Chinese military-civil fusion strategy: A state action theory perspective. *The International Spectator* 57 (3): 85–102.
Capri, A. 2020. Techno-nationalism: The US-China tech innovation race. New challenges for markets, business and academia. *Hinrich Foundation* 2020: 1.
Carter, W. (2018) Statement Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities, "Chinese Advances in Emerging Technologies and their Implications for US National Security". https://csis-website-prod.s3.amazonaws.com/s3fspublic/congressional_testimony/ts180109_Carter_Testimony.pdf
Castro, D., and M. McLaughlin. 2021. Who is winning the AI race: China, the EU, or the United States? 2021 update. *Center for Data Innovation* 2021: 1.
Castro, D., M. McLaughlin, and E. Chivot. 2019. Who is winning the AI race: China, the EU or the United States. *Center for Data Innovation* 2019: 1.
Cave, D., Hoffman, S., Joske, A., Ryan, F., and E. Thomas. 2019. Mapping China's Technology Giants.
Center for Security and Emerging Technology. 2021, May 13. China's 14th five-Year plan. https://cset.georgetown.edu/publication/china-14th-five-year-plan/
Cheung, R., and B. Wilhelm. 2020. The Worsening Rift Between Australia and China Is a Harbinger of Things to Come. https://www.worldpoliticsreview.com/trend-lines/29293/therift-in-australia-china-relations-is-a-ha rbinger-of-things-to-come
Chorzempa, M., and L.V. Daniels. 2023. New US export controls: key policy choices for Europe; recommendations for a robust European export control policy.
Christie, Ø.S., J. Jakobsen, and T.G. Jakobsen. 2023. The US way or Huawei? An analysis of the positioning of secondary states in the US–China rivalry. *Journal of Chinese Political Science* 2023: 1–32.
Chu, Y.H., L. Kang, and M.H. Huang. 2015. How east Asians view the rise of China. *Journal of Contemporary China* 24 (93): 398–420.
Cohen, J., and R. Fontaine. 2020. Uniting the techno-democracies: how to build digital cooperation. *Foreign Affairs* 99: 112.

Corcoral, M. 2021. Omnipresence without omnipotence: The US campaign against huawei in the 5G Era. *Conflicts, Crimes and Regulations in Cyberspace* 2: 117–146.

Corrado, J. 2023. 6 Strengthening the Indo-Pacific Chip Supply Chain. Indo-Pacific Strategies and Foreign Policy Challenges: The US-China Strategic Competition.

Coy, P. 2021. Onshoring is so last year. The new lingo is ‘friend-shoring’. Bloomberg EE. UU. Edition.

CSIS. 2023, March. Survey of Chinese espionage in the United States since 2000.csis.org/programs/strategic-technologies-program/archives/survey-chinese-espi onage-united-states-2000

CSIS. 2023, May 30. Securing Semiconductor Supply Chains in the Indo-Pacific Economic Framework for Prosperity. https://www.csis.org/analysis/securing-semiconductor-supply-chains-indo-pacific-economic-framework-prosperity

Culpan, T. 2019, May 20. The tech cold war has begun. Bloomberg.

Daniel Mügge (2023) The securitization of the EU’s digital tech regulation. *Journal of European Public Policy*, 30 (7): 1431–1446. https://doi.org/10.1080/13501763.2023.2171090

Disis, J. 2020. A new world war over technology. CNN. https://edition.cnn.com/2020/07/10/tech/us-china-global-tech-war-intl-hnk/index.html

Duchâtel, M. 2023. Europe’s China problem: How not to feed Beijing’s military-civil fusion. *Survival* 65 (4): 55–78.

Eckstein, H. 1975. Case studies and theory in political science. In *Handbook of political science*, vol. 7, ed. F. Greenstein and N. Polsby, 79–138. Reading, MA: Addison-Wesley.

Edwards, J., 2023. Chips, subsidies, security, and great power competition, Lowy Institute. Australia. Retrieved from https://policycommons.net/artifacts/3936589/chips-subsidies-security-and-great-power-competition/4742771/

Elman, C. (2003). Introduction: Appraising Balance of Power Theory. In *Realism and the Balancing of Power: A New Debate*, edited by Vasquez, J. A., and Elman, C. 1–22. Upper Saddle River, NJ: Prentice Hall.

Erlbacher, L., and S. Schmalz. 2023. Chinese perspectives on the US–China rivalry: navigating geo-economic and technological tensions in a new era of global statism. *Critical Policy Studies* 2023: 1–9.

Eslami, M., N.S. Mosavi, and M. Can. 2023. Sino-Iranian cooperation in artificial intelligence: A potential countering against the US hegemony. In *The Palgrave handbook of globalization with Chinese characteristics*, ed. P.A.B. Duarte, F.J.B.S. Leandro, and E.M. Galán. London: Palgrave.

European Commission, High Representative of the European Union for Foreign Affairs and Security Policy. (2023, June 20). ‘Joint Communication to the European Parliament, the European Council and the Council on “European Economic Security Strategy”. https://eurlex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023JC0020

European Parliament. (2020). COVID-19 foreign influence campaigns Europe and the global battle of narratives. Brussels. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649367/EPRS_BRI(2020)649367_EN.pdf

Fannin, R. 2020. How the US-China trade war has starved some Silicon Valley start-ups. https://www.cnbc.com/2020/01/31/chinese-venture-capitalists-draw-back-silicon-valleyinvestments.html

Feldstein, S. 2019. *The global expansion of AI surveillance*, vol. 17. Washington, DC: Carnegie Endowment for International Peace.

Financial Times. 2023, October 18. Five eyes spy chiefs warn Silicon Valley over Chinese threat. https://www.ft.com/content/0a37da0a-ad06-43d0-b069-bfafa0ff35a4

Fischer, S.C., and A. Wenger. 2021. Artificial intelligence, forward-looking governance and the future of security. *Swiss Political Science Review* 27 (1): 170–179.

Fischer, S. C. 2023. Silicon Curtain: America’s Quest for Allied Export Controls against China. In Strategic Trends 2023: Key Developments in Global Affairs (pp. 39–61). Center for Security Studies (CSS), ETH Zürich.

Fontaine, R. 2023, February 7. China’s balloon could be America’s awakening. Foreign Policy. https://foreignpolicy.com/2023/02/07/china-spy-balloon-us-national-security/

Ford, A. 2020, March 16. The PRC’s “Military-Civil Fusion” Strategy Is a Global Security Threat. https://2017-2021.state.gov/the-prcs-military-civil-fusion-strategy-is-a-global-security-threat/

Fricke, B. 2020. Artificial intelligence, 5G and the future balance of power. Konrad-Adenauer-Stiftung.

Friis, K., and O. Lysne. 2021. Huawei, 5G and security: Technological limitations and political responses. *Development and Change* 52 (5): 1174–1195.

Fuller, D. B. (2022). Weaponizing interdependence & global value chains: US export controls on Huawei. American Political Science Association pre-prints.

Global Innovation Index. 2022. What is the future of innovation-driven growth? Global Innovation Index. https://www.globalinnovationindex.org/Home
Goldman, D.P. 2020. *You will be assimilated: China's plan to sino-form the world*. London: Bombardier Books.
Goldman, E.O., and R.B. Andres. 1999. Systemic effects of military innovation and diffusion. *Security Studies* 8 (4): 79–125.
Goldstein, A. 2020. China's grand strategy under Xi Jinping: Reassurance, reform, and resistance. *International Security* 45 (1): 164–201.
Gorman, L. 2021, August 14. China's data ambitions: Strategy, Emerging Technologies, and implications for democracies. The National Bureau of Asian Research. https://www.nbr.org/publication/chinas-data-ambitions-strategy-emerging-technologies-and-implications-for-democracies/
Gray, J.E. 2021. The geopolitics of "platforms": The TikTok challenge. *Internet Policy Review* 10 (2): 1–26.
Greene, R., & Triolo, P. 2020. Will China Control the Global Internet Via its Digital Silk Road? Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-itsdigital-silk-road-pub-81857.
Greitens, S. C. (2020). Dealing with demand for China's global surveillance exports. Brookings Institution Global China Report.
Grochmalski, P., Lewandowski, P., & Paszak, P. (2020). US-China Technological Rivalry and its Implications for the Three Seas Initiative (3SI). European Research Studies Journal, 23(Special 2), 840–853.
Grotto, A., & Schallbruch, M. 2019, September 16. The great anti-china tech alliance. Foreign Policy. https://foreignpolicy.com/2019/09/16/the-west-will-regret-letting-china-win-the-tech-race/
Haas, M. C., & Fischer, S. C. 2020. The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order. In The Transformation of Targeted Killing and International Order (pp. 107–132). Routledge.
Han, Z., and T.V. Paul. 2020. China's rise and balance of power politics. *The Chinese Journal of International Politics* 13 (1): 1–26.
Harold, S., Beauchamp-Mustafaga, N., and J. Hornung. 2021. Chinese disinformation efforts on social media. https://www.rand.org/content/dam/rand/pubs/research_reports/RR4300/RR4373z3/RAND_RR4373z3.pdf
Hart, B., Lin, B., Lua, S., Price, H., Liao, G., & Slade, M. 2023, August 16. Is China a leader in Quantum Technologies? China Power Project. https://chinapower.csis.org/china-quantum-technology/
Harwit, E. 2023. U.S.-China 5G competition, the economy-security nexus, and Asia. *Journal of Chinese Political Science* 2023: 1–16.
He, K. 2012. Undermining adversaries: Unipolarity, threat perception, and negative balancing strategies after the cold war. *Security Studies* 21 (2): 154–191.
He, K., and H. Feng. 2012. 'Why is there no NATO in Asia?' revisited: Prospect theory, balance of threat, and US alliance strategies. *European Journal of International Relations* 18 (2): 227–250.
Heath, T.R., D. Grossman, and A. Clark. 2021. *China's quest for global primacy: An analysis of Chinese International and Defense Strategies to Outcompete the United States*. Santa Monica: RAND Corporation.
Heath, T. R. 2023, March 24. Why is China strengthening its military? it's not all about war. RAND Corporation. https://www.rand.org/blog/2023/03/why-is-china-strengthening-its-military-its-not-all.html
Heginbotham, E., Nixon, M., Morgan, F. E., Heim, J. L., Hagen, J., Li, S. T., and L. J. Morris. 2015. Chinese Attacks on US Air Bases in Asia: An Assessment of Relative Capabilities, 1996–2017. Santa Monica: Rand Corporation. https://www.rand.org/pubs/research_reports/RR392.html
Hillman, J.E. 2021. *The digital silk road: China's quest to wire the world and win the future*. London: Profile Books.
Horowitz, M. C. 2018. Artificial intelligence, international competition, and the balance of power.
Hotta, T. 2022, October 6. Why Japan remains the biggest investor in the US. Financial Times. https://www.ft.com/content/7d82485f-0668-4823-b9d3-ca59d6ad4913
Howell, S. 2023, January 13. The China-US quantum race. The Diplomat. https://thediplomat.com/2023/01/the-china-us-quantum-race/ https://asia.nikkei.com/Business/Tech/Semiconductors/Netherlands-unveils-chip-tool-export-curbs-in-fresh-blow-to-China

Huang, Y., & Slosberg, G. 2023, July 5. Europe narrowly navigates de-risking between Washington and Beijing. https://carnegieendowment.org/2023/07/05/europe-narrowly-navigates-de-risking-between-washington-and-beijing-pub-90131

Huang, Y., and M. Mayer. 2023. Power in the age of datafication: Exploring China's global data power. *Journal of Chinese Political Science* 28 (1): 25–49.

Imbrie, A., R. Fedasiuk, C. Aiken, T. Chhabra, and H. Chahal. 2020. Agile alliances: How the United States and its allies can deliver a democratic way of AI. *Center for Security and Emerging Technology* 2020: 1.

Inkster, N. 2019. The Huawei Affair and China's technology ambitions. *Survival* 61 (1): 105–111.

Iyengar, R. 2023, March 14. Is this Tiktok's Huawei Moment? Foreign Policy. https://foreignpolicy.com/2023/03/14/tiktok-ban-us-canada-eu-government/

Jarnceck, J., and S. Dawda. 2022. A Dual Approach to Tackling IP Theft and IP. RUSI. https://rusi.org/explore-our-research/publications/commentary/dual-approach-tackling-ip-theft-and-ip-loss

Jensen, B.M., C. Whyte, and S. Cuomo. 2020. Algorithms at war: The promise, peril, and limits of artificial intelligence. *International Studies Review* 22 (3): 526–550.

Ji, E. 2023, February 24. Great leap nowhere: The challenges of China's semiconductor industry. War on the Rocks. https://warontherocks.com/2023/02/great-leap-nowhere-the-challenges-of-chinas-semiconductor-industry/

Jiang, B. 2023, July 1. China's chip ambitions dealt fresh blow by new export rules on ASML machines. South China Morning Post. https://www.scmp.com/tech/tech-war/article/3226225/chinas-semiconductor-ambitions-dealt-fresh-blow-new-dutch-export-rules-asml-chip-making-machines

Johnson, J. 2020. Deterrence in the age of artificial intelligence & autonomy: A paradigm shift in nuclear deterrence theory and practice? *Defense and Security Analysis* 36 (4): 422–448.

Johnson, J., and E. Krabill. 2020. AI, Cyberspace, and nuclear weapons. War on the Rocks. https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons/

Johnson, M. 2023. China's Grand Strategy for Global Data Dominance. https://www.hoover.org/research/chinas-grand-strategy-global-data-dominance

Joseph Jarnecki and Sneha Dawda. 2022. A Dual Approach to Tackling IP Theft and IP Loss. RUSI. https://www.rusi.org/explore-our-research/publications/commentary/dual-approachtackling-ip-theft-and-ip-loss

Kahata, A. (2020) Assessing the Impact of U.S.-China Technology Competition and Decoupling: Focusing on 5G. Centre for Strategic International studies. https://www.csis.org/blogs/technology-policy-blog/assessing-impact-us-china-technologycompetition-and-decoupling

Kania, E., and L. Laskai. 2021. Myths and Realities of China's Military-Civil Fusion Strategy. CNAS. https://www.cnas.org/publications/reports/myths-and-realities-of-chinasmilitary-civil-fusion-strategy.

Kania, E. B., and W. VornDick. 2019. China's Military Biotech Frontier: CRISPR, Military-Civil Fusion, and the New Revolution in Military Affairs. China Brief.

Kania, E. 2017. Battlefield Singularity. Artificial Intelligence, Military Revolution, and China's Future Military Power, CNAS.

Kania, E.B. 2022. Artificial intelligence in China's revolution in military affairs. In Defence Innovation and the 4th Industrial Revolution (pp. 65–92). Routledge.

Khan, A. 2021. Kristen Hopewell, clash of powers: US–China rivalry in global trade governance. *Journal of Chinese Political Science* 2021: 1.

Kokas, A. 2022. *Trafficking data: How China is winning the battle for digital sovereignty*. Oxford: Oxford University Press.

Korolev, A. 2020. How closely aligned are China and Russia? Measuring strategic cooperation in IR. *International Politics* 57 (5): 760–789.

Krolikowski, A., and T.H. Hall. 2023. Non-decision decisions in the Huawei 5G dilemma: Policy in Japan, the UK, and Germany. *Japanese Journal of Political Science* 2023: 1–19.

Kuo. 2021. 'Clean Network' in the US-China Tech Race. The Diplomat. https://thediplomat.com/2021/03/clean-network-in-the-us-china-tech-race/

Lai, H. 2001. Behind China's world trade organization agreement with the USA. *Third World Quarterly* 22 (2): 237–255.

Laskai, L., and A. Segal. 2018, December 6. A new old threat: Countering the return of Chinese Industrial Cyber Espionage. Council on Foreign Relations. https://www.cfr.org/report/threat-chinese-espionage

Le Corre, P., and V. Vuksanovic. 2019. Serbia: China's open door to the Balkans. The Diplomat.

Lee, S.H. 2023. US semiconductor policy and South Korea: A delicate balancing act between national priorities and international collaboration. *Asia Policy* 30 (3): 101–127.
Lee, S. 2024. US–China technology competition and the emergence of techno-economic statecraft in East Asia: High technology and economic-security nexus. *Journal of Chinese Political Science* 2024: 1–20.
Lee, J., and R. Maher. 2022. US economic statecraft and great power competition. *Business and Politics* 24 (4): 332–347.
Lee, J.Y., E. Han, and K. Zhu. 2022. Decoupling from China: How US Asian allies responded to the Huawei ban. *Australian Journal of International Affairs* 76 (5): 486–506.
Leoni, Z. 2022. The End of the "Golden Era"? The Conundrum of Britain's China Policy Amidst Sino-American Relations. *Journal of Current Chinese Affairs* 51 (2): 313–326.
Levine, D.A. 2020. Made in China 2025. *Journal of Strategic Security* 13 (3): 1–16.
Lewis, J.A. 2019. Emerging technologies and managing the risk of tech transfer to China. *Center for Strategic & International Studies* 2019: 1.
Lewis, J.A. 2020. Managing Semiconductor Exports to China. Commentary. CSIS.
Li, J., J. Xia, and Z. Lin. 2017. Cross-border acquisitions by state-owned firms: How do legitimacy concerns affect the completion and duration of their acquisitions? *Strategic Management Journal* 38 (9): 1915–1934.
Lindsay, J.R., T.M. Cheung, and D.S. Reveron, eds. 2015. *China and cybersecurity: Espionage, strategy, and politics in the digital domain*. Oxford: Oxford University Press.
Liu, L. 2021. The rise of data politics: Digital China and the world. *Studies in Comparative International Development* 56: 45–67.
Liu, John, and Paul Mozur. "Inside Taiwanese Chip Giant, a U.S. Expansion Stokes Tensions." The New York Times, February 22, 2023.
Lobell, S.E. 2018. A granular theory of balancing. *International Studies Quarterly* 62 (3): 593–605.
Lorenzo, P., Stefano, F., Ferreira, A., and P. Carolina. 2021. Artificial intelligence and cybersecurity: Technology, governance and policy challenges (pp. 122). Centre for European Policy Studies.
Luo, Y. 2022. Illusions of techno-nationalism. *Journal of International Business Studies* 53: 550–567. https://doi.org/10.1057/s41267-021-00468-5.
Macias, A. 2019, July 24. New defense secretary: "We need to be very concerned about Chinese technology getting into our systems." CNBC. https://www.cnbc.com/2019/07/24/new-pentagon-chief-very-concerned-about-chinese-tech-getting-into-us-systems.html
Malkin, A., and T. He. 2023. The geoeconomics of global semiconductor value chains: extraterritoriality and the US–China technology rivalry. *Review of International Political Economy* 2023: 1–26.
Manuel, A., and K. Hicks. 2020. Can China's Military Win the Tech War? Foreign Affairs. https://www.foreignaffairs.com/articles/united-states/2020-07-29/can-chinas-military-wintech-war
Mark, J., and D. T. Roberts. 2023. United States-China semiconductor standoff: A supply chain under stress. Atlantic Council.
Mascitelli, B., and M. Chung. 2019. Hue and cry over Huawei: Cold war tensions, security threats or anti-competitive behaviour? *Research in Globalization* 2019: 1.
Mearsheimer, J. J. 2015. Why we will soon miss the Cold War. In Conflict after the cold war (pp. 28–44). Routledge.
Mehta, Rupal N. 2021. Extended deterrence and assurance in an emerging technology environment. *Journal of Strategic Studies* 44 (7): 958–982.
Milutinović, P., and G. Nikolić. 2023. Can China challenge the technological supremacy of the United States: current standpoint and perspectives. Review of International Affairs.
Mishra, M., P. Yan, and R. Schroeder. 2022. TikTok politics: Tit for tat on the India-China cyberspace frontier. *International Journal of Communication* 16: 26.
Mohamed, N.A., A. Jantan, and O.I. Abiodun. 2018. Protect governments, and organizations infrastructure against cyber terrorism (mitigation and stop of server message block (SMB) remote code execution attack). *International Journal of Engineering Research and Technology* 11 (2): 261–272.
Montgomery, E. B. 2017. US–China Competition in Defense Technological and Industrial Development: Implications for the Balance of Power over the Long Term. SITC Research Briefs (2017-13).
Moore, G.J. 2023. Huawei, cyber-sovereignty and liberal norms: China's challenge to the west/democracies. *Journal of Chinese Political Science* 28: 151–167.

Murphy, A., and H. Tucker. 2023, June 8. The global 2000. Forbes. https://www.forbes.com/lists/global2000/?sh=51ba54675ac0

Ng, K. 2023, March 7. Suppressing China won't make America great—Chinese foreign minister Qin Gang. BBC News. https://www.bbc.com/news/world-asia-china-64871808

Oikawa, A. 2019. Japan's R&D spending hits record for nearly half of companies: But nation still lags US and China in pace of innovation investments. *Nikkei Asian Review* 2019: 1.

Oxford Analytica. 2023. Five Eyes cyber plans will focus on Russia and China, Expert Briefings.

Papageorgiou, M.M. 2023. China's Growing Presence in the Middle East's Arms Race and Security Dynamics. In *The Arms Race in the Middle East Contributions to International Relations*, ed. M. Eslami and A.V. Guedes Vieira. Cham: Springer.

Papageorgiou, M., and D.D.S.N. de Melo. 2022. China as a responsible power amid the COVID-19 crisis: Perceptions of partners and adversaries on twitter. *Fudan Journal of the Humanities and Social Sciences* 15 (2): 159–188.

Papageorgiou, M., and A. Vieira. 2021. A friend in need? The Sino-Russian relationship under the coronavirus crisis in Twitter: A Russian perspective. *East Asia* 38 (3): 225–247.

Papageorgiou, M., and A. Vysotskaya Guedes Vieira. 2023. Assessing the Changing Sino–Russian Relationship: A Longitudinal Analysis of Bilateral Cooperation in the Post-Cold War Period. Europe-Asia Studies, 1–27.

Parameswaran, P. 2019. What's in the New US-Singapore Artificial Intelligence Defense Partnership? The Diplomat.

Paszak, P. 2019. China's technological transformation and the future of Sino-American competition. *Polish Journal of Political Science* 5 (2): 87–116.

Patil, Krutika. 2022. "Quad and Cybersecurity." Manohar Parrikar Institute for Defence Studies and Analyses. June 22. https://idsa.in/idsacomments/quad-and-cybersecurity-kpatil-220622.

Payne, K. 2018. Artificial intelligence: A revolution in strategic affairs? *Survival* 60 (5): 7–32.

Pecotic, A. 2019, March 5. Whoever predicts the future will win the AI Arms Race. Foreign Policy. https://foreignpolicy.com/2019/03/05/whoever-predicts-the-future-correctly-will-win-theai-arms-race-russia-china-united-states-artificial-intelligence-defense/. POLITICO. https://www.politico.eu/article/countries-push-back-against-uss-anti-china-tech-policy

Pollet and Handel (2023, November 2023). The West is on a world tour against Huawei. The West is on a world tour against Huawei – POLITICO

Qi, Z. 2023. US technological decoupling from China: Strategic motives and policy measures. *China Int'l Stud.* 98: 101.

Qiao-Franco, G., and I. Bode. 2023. Weaponized artificial intelligence and Chinese practices of human–machine interaction. *The Chinese Journal of International Politics* 16 (1): 106–128.

Qiu, J.L. 2023. The return of billiard Balls? US–China Tech War and China's State-Directed Digital Capitalism. *Javnost-the Public* 30 (2): 197–217.

Raymer, M. G., & Monroe, C. (2019). The US national quantum initiative. *Quantum Science and Technology* 4 (2): 020504.

Richmond, T. 2023, January 24. Explainer: University of Wisconsin latest to Ban Tiktok. AP News. https://apnews.com/article/technology-politics-united-states-government-china-privacy-26b0ee0d4c8421fa7f58b06f76651dc1

Rim, H. J. 2023. The US–China Strategic Competition and Emerging Technologies in the Indo-Pacific Region: Strategies for Building, Dominating, and Managing Networks. Indo-Pacific Strategies and Foreign Policy Challenges, 60–78.

Ross, R. S. (2006). Balance of power politics and the rise of China: Accommodation and balancing in East Asia. *Security Studies* 15 (3): 355–395.

Rotolo, D., D. Hicks, and B.R. Martin. 2015. What is an emerging technology? *Research Policy* 44 (10): 1827–1843.

Roy, D. 2005. Southeast Asia and China: Balancing or bandwagoning? *Contemporary Southeast Asia: A Journal of International and Strategic Affairs* 27 (2): 305–322.

Rydning, D.R.J.G.J., J. Reinsel, and J. Gantz. 2018. The digitization of the world from edge to core. *Framingham: International Data Corporation* 16: 1–28.

Saltzman, I.Z. 2023. Diversionary words: Trump, China and the COVID-19 Pandemic. *Chinese Political Science Review* 2023: 1–25.

Satoru, M. 2021. The Biden Administration's First Year in the Indo-Pacific: Balancing, Order-Building and Managing Competition with China. *Asia-Pacific Review* 28 (2): 77–106.

Satu Limaye and Rose Tenyotkin. 2021. Maintaining the Technology Edge: Strengthening US and Indo-Pacific Alliances to Counter Chinese Technology Acquisition. Center for Naval Analyses. Maintaining the Technology Edge: Strengthening US and Indo-Pacific Alliances to Counter Chinese Technology Acquisition | CNA
Scharre, P. 2019. Killer apps: The real dangers of an AI arms race. *Foreign Affairs* 98: 135.
Scharre, P. 2023. Four battlegrounds: power in the age of artificial intelligence. HighBridge Audio.
Schmidt, E. 2022. AI, great power competition & national security. *Daedalus* 151 (2): 288–298.
Scott, M., and B. Bordelon. 2023, June 15. Countries push back against US's anti-China Tech policy.
Sechser, T.S., N. Narang, and C. Talmadge. 2019. Emerging technologies and strategic stability in peacetime, crisis, and war. *Journal of Strategic Studies* 42 (6): 727–735.
Segal, A. 2019. Seizing core technologies: China responds to US technology competition. *China Leadership Monitor* 60: 1–12.
Selden, Z. 2013. Balancing against or balancing with? The spectrum of alignment and the endurance of American hegemony. *Security Studies* 22 (2): 330–364.
Semiconductor Industry Association. 2022, October. 2022 State of the US Semiconductor Industry. https://www.semiconductors.org/wp-content/uploads/2022/11/SIA_State-of-Industry-Report_2022.pdf
Shah, A.R. 2023. Revisiting China threat: The US' securitization of the 'Belt and Road Initiative.' *Chinese Political Science Review* 8 (1): 84–104.
Shahbaz, A. 2018. The Rise of Digital Authoritarianism. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism
Sheehan, M. 2022, October 27. Biden's unprecedented semiconductor bet. Carnegie endowment. https://carnegieendowment.org/2022/10/27/biden-s-unprecedented-semiconductor-bet-pub-88270
Shifrinson, J. 2018. Should the United States fear China's rise? *The Washington Quarterly* 41 (4): 65–83.
Shi-Kupfer, K., and M. Ohlberg. 2019. China's digital rise. MERICS. MERICS. https://merics.org/en/report/chinas-digital-rise
Slotta, D. 2023, January 24. China: Growth rate of big data industry. Statista. https://www.statista.com/statistics/1284407/china-growth-rate-of-big-data-industry/
Smith-Goodson, P. 2019. Quantum USA vs. Quantum China: The World's Most Important Technology Race. Forbes. https://www.forbes.com/sites/moorinsights/2019/10/10/quantumusa-vs-quantum-china-the-worlds-most-important-technology-race/?sh=483a7fa872de.
Snyder, G.H. 1991. Alliances, balance, and stability. *International Organization* 45 (1): 121–142.
Snyder, Glenn. 1997. *Alliance Politics*. Ithaca and London: Cornell University Press.
Stanford University Human Centered Artificial Intelligence. (2022). The AI index report 2022—Artificial Intelligence Index. https://aiidex.stanford.edu/ai-index-report-2022/
Starr, H. 2005. Territory, proximity, and spatiality: The geography of international conflict. *International Studies Review* 7 (3): 387–406.
Steff, R., J. Burton, and S.R. Soare. 2020. *Emerging technologies and international security*. London: Routledge.
Sun, H. 2019. US-China tech war: Impacts and prospects. *China Quarterly of International Strategic Studies* 5 (02): 197–212.
Swanson, A., Mozur, P., and R. Zhong. 2020. U.S. Is Using Taiwan as a Pressure Point in Tech Fight with China. https://www.nytimes.com/2020/05/19/business/economy/chinataiwan-huawei-tsmc.html
Tang, F. 2023, February 2. China must be a world leader in science and Tech or risk being "strangled": Xi. South China Morning Post. https://www.scmp.com/economy/china-economy/article/3208882/xi-jinping-says-china-must-quicken-pace-tech-self-reliance-prevent-being-strangled-foreign-countries
Taylor, M. 2022. China's digital authoritarianism goes global. In China's digital authoritarianism: A governance perspective. pp. 111–130. Cham: Springer.
The State Council of the People's Republic of China. (2015, September 5). Action Plan for Promoting Big Data Development. www.gov.cn.https://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm
The United States Congress. 2023, March 7. S.686- RESTRICT ACT 118th congress (2023–2024). https://www.congress.gov/bill/118th-congress/senate-bill/686
The United States Trade Representative. 2018, March 22. Findings of the investigation into China's acts, policies (….). https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF
The Wall Street Journal. https://www.wsj.com/articles/u-s-china-tech-fight-opens-newfront-in-ethiopia-11621695273

Thomala, L.L. 2023, April 19. Number of internet users in China 2022. Statista. https://www.statista.com/statistics/265140/number-of-internet-users-in-china/#:~:text=China's%20internet%20population%20grew%20by,fast%2Dgrowing%20mobile%20app%20market.&text=In%202022%2C%20China%20accounted%20for,5.3%20billion%20internet%20users%20worldwide.
Ting-Fang, C., and L. Li. 2023, June 30. Netherlands unveils chip tool export curbs in fresh blow to China. Nikkei Asia.
Torreblanca, J.-I. and R. Jorge-Ricart. 2022. The US-EU Trade and Technology Council (TTC): State of Play, Issues and Challenges for the Transatlantic Relationship.
Triolo, P. 2023. Technology crossroads: innovation in China's telecommunications and high-performance computer sectors threatened by US stranglehold on semiconductors. *Asian Security* 2023: 1–16.
United Nations Conference on Trade and Development. 2023. Technology and innovation report 2023. UNCTAD. https://unctad.org/tir2023
US Department of State. 2020, 16 March. The PRC's "Military-Civil Fusion" Strategy Is a Global Security Threat. https://2017-2021.state.gov/the-prcs-military-civil-fusion-strategy-is-a-global-security-threat/
USA Embassy in Georgia. 2020, 8 May. Briefing with special envoy Lea Gabrielle. https://ge.usembassy.gov/briefing-with-special-envoy-lea-gabrielle-global-engagementcenter-update-on-prc-efforts-to-push-disinformation-and-propaganda-around-covid-may-8/
USCC (2018). US-China Economic, & Security Review Commission. *Report to Congress of the US-China Economic and Security Review Commission*. https://www.uscc.gov/annual-report/2018-annualreport-congress
Van der Linden, R.W. and P. Łasak. 2023. The Ongoing Sino-US Trade War and Subsequent Tech War. In: Financial Interdependence, Digitalization and Technological Rivalries. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-27845-7_8
Walt, S. 1985. Alliance Formation and the Balance of World Power. *International Security* 9 (4): 3–43.
Walt, S.M. 1987. *The Origins of Alliances*. Ithaca, NY: Cornell University Press.
Walt, S.M. 1988. Testing theories of alliance formation: the case of Southwest Asia. *International Organization* 1988: 275–316.
Walt, S.M. 1992. Alliances, threats, and US grand strategy: A reply to Kaufmann and Labs. *Security Studies* 1 (3): 448–482.
Walt, S.M. 2009. Alliances in a Unipolar World. *World Politics*. 61 (3): 86–120.
Wang, Y., and D. Chen. 2018. Rising Sino-US competition in artificial intelligence. *China Quarterly of International Strategic Studies* 4 (02): 241–258.
Wang, D. 2023, February 28. China's Hidden Tech Revolution. Foreign Affairs. https://www.foreignaffairs.com/china/chinas-hidden-tech-revolution-how-beijing-threatens-us-dominance-dan-wang
Whalen, J. 2019. Chinese scientists are at the forefront of the quantum revolution. The Washington Post. https://www.washingtonpost.com/business/2019/08/18/quantumrevolution-is-comingchinese-scientists-are-forefront/.
White House. 2018, October 4. Remarks by Vice President Pence on the Administration's Policy Toward China. National Archives and Records Administration. https://trumpwhitehouse.archives.gov/briefings-statements/remarks-vice-president-pence-administrations-policy-toward-china/
White House. 2020. United States Strategic Approach to the People's Republic of China. https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.24v1.pdf
White House. 2021a, June 3. Executive order on addressing the threat from securities investments that finance certain companies of the People's Republic of China. White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/executive-order-on-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/
White House. 2021b, June 9. Executive order on protecting Americans' sensitive data from foreign adversaries. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/
White House. 2022a, April 5. Fact sheet: Implementation of the Australia—United Kingdom—United States Partnership (AUKUS). White House. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/
White House. 2022b, August 9. Fact sheet: Chips and science act will lower costs, create jobs, strengthen supply chains, and Counter China. White House. https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

Wilkins, T.S. 2012. ‘Alignment’, not ‘alliance’—The shifting paradigm of international security cooperation: Toward a conceptual taxonomy of alignment. *Review of International Studies* 38 (1): 53–76.
Williams, M.A. 2019. The artificial intelligence race: Will Australia lead or lose? *Journal and Proceedings of the Royal Society of New South Wales* 152 (471/472): 105–114.
Williamson, P., and A. Raman. 2011. The global: How China reset its global acquisition agenda. *Harvard Business Review* 89 (4): 109–114.
Woo, S., and A. Wexler. 2021, May 22. U.S.-China tech fight opens new front in Ethiopia.
Wu, X. 2020. Technology, power, and uncontrolled great power strategic competition between China and the United States. *China International Strategy Review* 2 (1): 99–119.
Wu, D., Hoenig, H., and H. Dormido. 2019. Who’s winning the tech Cold War? A China vs. US scoreboard. Bloomberg.
Xin Liu. 2021. Chinese Multinational Enterprises Operating in Western Economies: Huawei in the US and the UK. *Journal of Contemporary China* 30 (129): 368–385. https://doi.org/10.1080/10670564.2020.1827351
Yang, M., and P. Deng. 2017. Cross-Border M&As by Chinese companies in advanced countries: Antecedents and implications. *Thunderbird International Business Review* 59 (3): 263–280.
Yasir, S., and H. Kumar. 2020. India Bans 118 Chinese Apps as Indian Soldier Is Killed on Disputed Border. https://www.nytimes.com/2020/09/02/world/asia/india-bans-chinaapps.html
Yeung, H.W.C. 2022. Explaining geographic shifts of chip making toward East Asia and market dynamics in semiconductor global production networks. *Economic Geography* 98 (3): 272–298.
Yilmaz, S., and T. Sun. 2023. The China–US great power rivalry and the new anarchy. *Chinese Political Science Review* 8 (4): 507–526.
You, H. 2021. Semiconductors and the US China Innovation Race. Foreign Policy. Available: https://www.foreignpolicy.
Zaveri, P. 2023, January 7. Why India banned tiktok—And what the US can learn from it, as pressure mounts for Biden to follow suit. Business Insider. https://www.businessinsider.com/why-did-india-ban-tiktok-us-states-fcc-government-2023-1.
Zhang, Y. 2021. ‘Barbarising’ China in American trade war discourse: The assault on Huawei. *Third World Quarterly* 42 (7): 1436–1454.
Zhang, B., J. Zhang, and F. Yao. 2006. Technology transfer from the Soviet Union to the People’ Republic of China: 1949–1966. *Comparative Technology Transfer and Society* 4 (2): 105–167.
Zhang, Q., F. Xu, L. Li, N.L. Liu, and J.W. Pan. 2019. Quantum information research in China. *Quantum Science and Technology* 4 (4): 1.

Maria Papageorgiou is Lecturer in Politics and International Relations at the University of Exeter. Before that she has worked at UCL, SOAS University of London and Bradford University. She has also been visited researcher at St Petersburg University in Russia, Newcastle University, UK, ICD in Berlin, Germany, Institute of International Economic Relations, Athens, Greece and at the University of Maribor, Slovenia. Her research interests focus on International Relations theory, Sino-Russian relations, interstate relations in social media and emerging technologies while she also has expertise in quantitative research methods. She has published in various journals and think tanks among them in Europe Asia studies, International Affairs, Fudan Journal of Humanities and Social Sciences, Journal of Chinese Political Science, East Asia and Participation and Conflict among others.

Muhammed Can is PhD candidate of Political Science and International Relations at the University of Minho, Portugal. He holds a bachelor’s degree of Economics from Selçuk University, Turkey. He completed his postgraduate studies both at the Swansea University (International Relations) and King’s College London (Espionage and Surveillance Studies), UK. Previously he was a visiting PhD researcher at King’s College London (War Studies department) and currently he is collaborative member of the Research Centre in Political Science (CICP) at the University of Minho. His research focuses on artificial intelligence, irregular warfare, intelligence and counterintelligence, special operations, and Chinese politics.

Alena Vieira Alena Vysotskaya Guedes Vieira is Assistant Professor at the University of Minho, Portugal, and Integrated Member of the Research Centre for Political Science (CICP). She holds an PhD in Political Science from the University Erlangen-Nürnberg, Germany. She was Visiting Researcher at the Finnish Institute of International Affairs, Instituto Estudos Estratégicos e Internacionais (Lisbon), and the University of Leuven. She has been granted scholarships and research grants by Chair InBev-Baillet Latour; Hanns-Seidel-Stiftung; Haniel-Stiftung; Compania di San Paulo, Riksbankens Jubileumsfond and Volkswagen-Stiftung, as well as Fundação para Ciência e Tecnologia. Her book "Russland, Belarus und die EU-Osterweiterung" was published by Ibidem-Verlag (2009), and she has also published in Journal of Common Market Studies, Europe-Asia Studies, Post-Soviet Affairs, Cambridge Review of International Affairs, International Spectator, among other journals. Alena Vieira has also published various policy briefs and reports for EU Institutions and think tanks. (orcid: 0000-0002-5643-0398).