Polish Political Science Yearbook, vol. 50(1), 2021, pp. 43–69
DOI: https://doi.org/10.15804/ppsy202116 PL ISSN 0208-7375
www.czasopisma.marszalek.com.pl/10-15804/ppsy

Karina Verónica Val Sánchez
Selcuk University-Konya (Turkey)
ORCID: 0000-0002-7036-3523
e-mail: kafkakun@gmail.com

Nezir Akyesilmen
Selcuk University-Konya (Turkey)
ORCID: 0000-0001-8184-5280
e-mail: nezmen@yahoo.com

Competition for High Politics in Cyberspace: Technological Conflicts Between China and the USA

Abstract: This paper highlighted the use of cyberspace as a conflict zone by the US and China, focusing on competition in various technological spheres, including cyberespionage, military technology, and Artificial Intelligence (AI). The main purpose of this study was to depict how great powers manipulate the cyber domain for their high political objectives through US-China rivalry. The research has been carried out mainly via literature review, discourse analysis, and relevant statistics. Consistent with previous literature and global public perception, the outcome has shown that both states are using cyberspace as a new domain for completion in trade, technology, and military purposes. Cyberespionage, the militarization of cyberspace, and AI have been the main conflict areas between these two global competitors in the last decade.

Keywords***:*** *USA, China, militarization of cyberspace, Artificial Intelligence, cyberespionage*

Introduction

As a new field of conflict in international relations (Akyesilmen, 2019), cyberspace has become a contested domain, a critical battleground for the United States and China in the last decade. The increase of cyber interactions between Washington and Beijing in this domain provides us with enough information to analyze the motivation for competition between these two powerful states. As a matter of fact, both countries have ambitions for wide-ranging and rapid military modernization implementing new technologies and cyber capabilities.

Relations between China and the United States from 1989 to 2016 went through a period of deepening and engagement, this period was mostly stable, and the United States showed a consistent foreign policy throughout the period. During the Obama administration, the first sign of change occurred when China proposed a "new type of major power relations". The Obama administration reacted in a reserved manner to the Beijing proposal. However, it became more evident in the second period of his administration that the proposal was completely rejected, and bilateral differences on issues such as the militarization of the South China Sea, trade deficits, and cyber-attacks began to gain more influence on the type of bilateral relationship. The transformation of US policy towards China was completed during the 2016 US presidential elections, and the subsequent victory of Donald Trump led to a new direction in the relationship with China. Differences became evident, and few paths to the resolution were proposed (Sutter, 2017). The current confrontation is depicted in actions and the discourse of politicians and high-level officials. Jisi notes that US rhetoric and actions toward China had not been as "aggressively and blatantly negative" (Jisi, 2020) as they are now when US policy toward China emphasizes rivalry and competition.

The military and technological empowerment that China is experiencing and the growing participation of the Communist Party in the economy and influence in society are the main triggers of American hostility towards China because they perceive a threat to both their interests and American values (Jisi, 2020). Consequently, the US administration has developed new strategies to address China's increased cyber competition, particularly in artificial intelligence and cyber-intelligence activities.

This study tries first to answer the question of "Is China going to win cyber power politics competition with the US?". The sub-questions are, but not limited to; what are the tools used in these cyber conflicts? What are their grand strategies? Who has the advantage? What is the role of R&D and private companies in this competition?

This work focuses on the nature of the conflict between the US and China, whether it is an economic or a military one, after a literature review session. Then it tries to elaborate on how cyberspace becomes a battlefield for the two rivals. It then discusses competition in AI, cyberespionage, and militarization of cyber domain by them. Finally, before the concluding remarks, it evaluates parties' position regarding technical education, R&D, and the private sector in their power struggle in cyberspace.

Literature Review

In recent years relations between China and the US have slid into strategic and technological competition and rivalry. There is plenty of literature coming out from these discussions in recent the decade. The majority of the literature focuses on confrontation, but a minority is facing the other way.

Jisi and Ran (2019) point out that the China-US relationship has been deteriorating in several dimensions. For instance, geostrategy, ideology, economics, and security issues have suffered considerable alterations since 2017. For the authors, in 2019 in both China and the United States, alarm bells went off predicting that the relationship had moved towards "long-term, full-scale confrontation". Jisi and Ran predict that in the years to come, the relationship will continue to spiral out of control if there is no reversal in the policies they are developing.

Mori (2019) argues that the administrations before Trump had followed an approach of commitment to China, but that the irruption of advanced technologies on the international scene has activated a relationship of competitive approach, making both countries maintain a constant exchange of efforts-countermeasures as they are immersed in "contest for supremacy over the next generation of military, economic and information/data dominance". Aaron Friedberg (2015) considers that the US has followed two strategies towards China, first, a strategy of engagement in a wide variety of areas, and second, a push-back strategy to stop China's growing strength. Zhao (2019) comments upon the Chinese Perspectives on US-China Strategic. The author expresses the growing concern within the political and intellectual elite about the possibility that competition between the United States and China will result in a cold war. Zhao also states that competition is inevitable because the national power gap between the two countries decreases and that ideological differences can increase competition in the bilateral relationship, which already has many aspects in dispute. In contrast to most Western scholars, Chinese strategists point out that competition also occurs in aspects such as prestige and international leadership, but they also recognize that economic and technological competition has increased. Lau (2020) makes an extensive analysis of the China-US trade war. In her article, she states that technological competition is taking place.

The most sensitive region under US-China competition is Asia-Pacific. Therefore several analysts comment on this. Shifrinson (2020) rejects that China will adopt an increasingly ambitious strategy; on the contrary, the interests shared with the US in the Asia-Pacific region will lead them to a cooperative relationship in the region. However, Noguchi (2011) is of the opposite opinion. He suggests that China's rapid growth rate of military expenditure is evidence that it is pursuing a more offensive approach in the region. Copeland (2012) comments that two great powers with strong interests in one region – Asia-Pacific – is dangerous and destabilizing. Yet, this position is nothing new, Bernstein and Munro (1997) had already pointed it out. The authors mentioned that the long-term confrontation of interests in the region could lead to a severe mutual conflict.

Several analysts put forward that China's growing military power is a critical threat to the United States. Saunders and Bowie (2016) state that cooperation between both nations is very difficult, mainly in the military sphere. In order to deter China's military dominance, Simón (2020) comments that Washington has adopted a flexible strategy that is even operationally contradictory when opting for deterring China through punishment and denial in both cases. The strategy is based on military-technological advantages that the United States has. Erickson and Goldstein (2006) claim that the United States must prioritize maintaining military forces to confront China because the intention to challenge US hegemony cannot be ruled out.

Innovation Imperative: A Power Transition in Progress?

In International Relations, several narratives have been gaining strength in recent years regarding the possible change in the international system from a unipolar to a multipolar order. The main premise is the weakening of US hegemony (Layne, 2012). Regarding this narrative, there are different positions; there are the denialists, the accepters, and the resisters. The first reject the weakening of US hegemony. The second recognizes that the rise of the rest is inescapable. Finally, some recognize that the United States is in a great powers-competition and could retain its position (Johnson, 2019b, pp. 4-5). Since the United States became the hegemonic leader within a unipolar international order at the end of the Cold War, each of the administrations which it has governed has set out to preserve American hegemony. Thus, it is possible to identify this aim as its grand strategy (Layne, 2012).

The order in the international system is changing. Russia and China are competing closely with the US. Yan Xuetong (2019) comments on two types of international engagement that China could follow and that are inspired by ancient Chinese philosophers, contrary to current proposals rooted in Western thought, where the prospects are for China to adopt the current liberal system or behave as a "revisionist power". He mentions that nations seek the respect of their international counterparts that exercise 'human authority', but there are nations who are a threat to their neighbors these nations exercise 'hegemony'. Also, he expresses the importance of leadership for the rise to power because there is a competition that pursues to gain international legitimacy. Therefore, moral leadership is preferable because it gives high strategic credibility and conducts policies with consistent moral standards (Pu, 2019). He believes that China can aspire to 'human authority', but some changes are needed. Because so far China's relationship with its neighbors is based on fear, the Communist Party's ideology is not shared by the citizens, and the "win-win" discourse presented by leader Xi Jinping lacks credibility as long as the abuse of citizens continues (Nyrén, 2019).

For many decades, the United States used its superiority in science and technology to ensure its hegemony, but today these powers also want to exploit it and bring about a shift in the balance of power. In this respect, Drezner (2001, p. 4) argues that "countries acquire hegemonic status because they are the first to develop a cluster of technologies in leading sectors" innovations impact the domestic economy and then impact internationally. When the hegemonic power slows down its innovation rate, it enters a period of struggle with the fast follower powers until a new 'technological hegemons' is found. In addition, the dominant power fears that "the other superpower might achieve a significant technological breakthrough and seek to exploit it" (Gilpin, 1988, p. 162). Taken together, these contributions suggest that the hegemonic power needs to maintain an advantage and superiority technologically against the powers that challenge its dominant position; otherwise, its position may be jeopardized (Deutch, 2018).

Lim and Kennedy's work focuses particularly on analyzing the interaction between great powers, mainly on how technology and innovation create a rivalry between the dominant state and the rising power (Kennedy & Lim, 2018, pp. 553-572). Economic superiority is one of several elements that drive the rise of ascending power. Yet, in the long run, economic development is maintained through technological innovation, which "generate spillover effects to the rest of the lead economy and then to the global economy" (Drezner, 2001). The innovation imperative is when the rising power tries to acquire or create new technology to ensure its rise. In the process, it develops strategies and policies to acquire and develop technologies, but especially increases spending on research and development (Kennedy & Lim, 2018).

As a rising power, China needs to create new products and get new technology (Reuveny & Thompson, 2001). There are three ways in which technology is acquired: making, taking, and transacting. Taking involves non-transactional means. Making is the result of supporting local producers in creating new ones. Transacting is a commercial exchange of technology (Kennedy & Lim, 2018, pp. 556-557). In this sense, it is necessary to mention that China has no complex about the idea of copying inventions, products, or technologies in order to benefit from technological advances quickly (Lee, 2018, pp. 29-55). The United States has also highlighted the successful and constant attempts by Chinese hackers to access the American network in search of possible technological secrets (Segal, 2016, pp. 119-122). Some have even commented that Chinese military equipment is very similar to that of the United States (Segal, 2016, p. 120).

China and the United States are the world's largest investors in research and development (R&D). However, the American model of innovation is subordinated to federal support, so it is alarming that in recent years federal support for R&D has declined and especially at a time of global competition where it is estimated that by 2030 China will be the country that invests the most in R&D (McRaven, 2019, 5) surpassing the US An insightful report by the Council on Foreign Relations (CFR) recommends that the US government should increase funding from 0.7% to 1.1% of gross domestic product (GDP) annually (McRaven, 2019: 6) so that the US does not lose its technological advantage and has a greater involvement as the private sector is currently at the forefront (Glosserman, 2020).

The actions of the ascending power unleash two types of effects concerning the dominant power: which firstly experiences a threat to its national security (security externalities) and subsequently to its position in the international system (order externalities) (Kennedy & Lim, 2018, pp. 553-555). As mentioned in the first part, the US NDS states that China is a threat to the current order of the international system (order externalities) (Mattis, 2018, p. 2). Also, China's ambitions to access emerging technologies with military applications are also perceived as a threat to US national security (security externalities). China wants to catch up with the United States in military technology and eventually overcome it (Mori, 2018, p. 2). Both the United States and China compete to dominate militarily exclusive breakthrough technology because it could shape next-generation military capabilities (Mori, 2018, p. 22).

The growing techno-rivalry has motivated both powers to adopt a techno-nationalist approach to maximize their national power. As China's supreme leader, Xi Jinping is convinced that the technological backwardness experienced in the past as a nation is rooted not in the lack of knowledge but the lack of its application for social and economic development (Xi, 2014). That is why he has focused on removing institutional barriers "to unleash to the greatest extent the huge potential of science and technology as the primary productive force" (Xi, 2014). Xi also stated the urgency of seizing the moment to take advantage of technology "I have repeatedly said that the great rejuvenation of the Chinese nation can in no way be realized easily. In fact, the stronger we become, the greater resistance and pressure we will encounter. That is why we say that timing and resolution are vital, as historical opportunities are often ephemeral. Now we have an important historic opportunity to promote scientific and technological innovation. We must not miss it, but seize it tightly" (Xi, 2014).

Xi Jinping is sure that a nation with technological inferiority is catastrophic for the total fulfillment of the Chinese dream (Paul, 2020). That is why he is working on initiatives that will lead the nation towards the fulfillment of that dream and to realize the Two Centenary Goals (Xi, 2014), namely 'Belt and Road Initiative' and 'Made in China 2025'.

A) 'Belt and Road Initiative' (BRI)

It was 2,100 years ago, during the Han Dynasty when the silk road began. However, it was not until 2013 that Jinping presented a modern route: Silk Road Economic Belt and the 21st Century Maritime Silk Road. A first glance suggests that it is a route connecting China to the rest of the world (more than 60 countries), but in fact, it is a broader proposal that involves many variables aligned to achieve long-term interest (Yunling, 2015). According to Jinping, One Belt and One Road (OBOR) "represent paths towards mutual benefit which will bring about closer economic integration among the countries involved, promote the development of their infrastructure and institutional innovation, create new economic and employment growth areas, and enhance their capacity to achieve endogenous growth and to protect themselves against risks." (Xi, 2014, p. 339).

B) Made in china 2025 (MIC2025)

Since its proposal in 2015, MIC2025 represents China's industrial policies for the next decade. The central axis is China's transformation into a global technology power (Chen et al., 2020). Hence, it is necessary to integrate advanced manufacturing techniques into the manufacturing industry. This sector is one of the largest in the world and faces serious problems of technology and innovation; therefore, there are many backward industries. MIC2025 seeks to mitigate these deficiencies through a megaproject approach (Lin, 2020). Also, MIC2025 sketches out a three-step strategy to upgrade the Chinese manufacturing industry towards an "industry 4.0" 1) innovation and efficient manufacturing processes to achieve industrialization by 2025. 2) China should be at the level of the manufacturing base of developed countries to compete with them by 20235. 3) China will be a manufacturing superpower. For the latter strategy, MIC2025 establishes clear principles, goals, instruments, and specific industries (Cheung et al., 2016). For instance, it has five sub-plans aimed at facilitating government participation: Manufacturing innovation center construction plan, Intelligent manufacturing plan, Core industrial capability strengthening plan, Green manufacturing plan, High-end equipment innovation plan. Also, it stresses ten priorities industrial areas among them agricultural equipment, aerospace, biomedical, railway, marine engineering and ships, new energies, new materials, power generation equipment, and of course automated machine tools and robotics and the new generation of information and communication technology (ICT), which will focus on three main technological areas: microchips and related hardware, information and communication devices, and industrial processing systems and software. These last two industrial priorities are particularly relevant to technological competition.

Can the United States deter Beijing's techno-nationalist ambitions? It depends on the seriousness of the Chinese challenge (Bey, 2018, p. 33). China is strongly responding to an innovation imperative as a rising power, putting forward strategies and plans to be able to obtain, make and take technologies (Kennedy & Lim, 2018). MIC2025 is the route the Chinese government has set out to achieve "self-sufficiency" and become a "manufacturing superpower" (Laskai, 2018b). As expected, this plan has been highly criticized by the US government. If China continues its technological push as it has so far, US superiority will likely extend for another decade until it is finally surpassed (Rasser, 2020).

Nature of the Conflict: Low or High Politics?

The Donald Trump administration has published two documents highlighting the international scenario that the United States is facing and the necessary actions to be taken. The first document is the 2017 National Defense Strategy (NDS) and 2018 National Security Strategy (NSS). In these documents is possible to identify a particularity that articulates both strategies: the return of great power competition (Trump, 2017, p. 27). The United States is involved in a great-power competition with China and Russia, and today it is the biggest national security threat they have to face (Mattis, 2018, p. 1), displacing the threat of terrorism into the background. Strategic competition is the best way to avoid large-scale conflicts (Blankenship & Denison, 2019, pp. 43-44), and to face this competition, it is necessary to maintain political, economic, military, and technological advantages (Trump, 2017, p. 3), because "every domain is contested—air, land, sea, space, and cyberspace" (Grieco, 2018, p. 3). Swaine (2018, p. 55) argues that the Chinese authorities very badly received these documents because the US "ignore Beijing's supposedly cooperative, win-win approach and peaceful intentions" (Swaine, 2018, p. 55).

The NDS (2017) and the NSS (2018) are major shifts in US foreign policy. Distinguishing it diametrically from the foreign policy that the Obama administration had towards Russia, but especially towards China "shifting from an engagement-based approach toward a competition-based one" (Mori, 2019, p. 77). This change in approach is mainly motivated by the prolonged and failed US strategy towards China (Friedberg, 2018, pp. 15-17).

These documents serve as policy guidance for specific US national security and defense priorities. In both documents, Beijing represents a competitor and a threat to US prosperity and security. In this sense, following a competition-based approach, it is possible to identify three shifts towards China under the Trump administration:

First, the US government has begun to operate in a very coordinated way to address the unfair acts of Beijing, namely forced technology transfer, intellectual property theft, cyberespionage, cyber-theft, market access, and the large trade imbalance in China's favor (Lau, 2020, pp. 32-34). For instance, the United States, through the Committee on Foreign Investment in the United States (CFIUS), has prevented investment in American technology companies by the Chinese venture capital firm. The power granted to this Committee by the Foreign Investment Risk Review Modernization Act (FIRRMA) is that it is even allowed to directly block potential purchases and investigate foreign entities. One of the most notorious cases is the blockade that the CFIUS made to prevent the purchase of US Lattice Semiconductor, which produces chips for the development of artificial intelligence technology (Hoadley & Lucas, 2018, p. 11). According to the White House, the purchase was blocked because its sale carries a national security risk due to Beijing's support for the operation (Johnson, 2019a, p. 10).

Second, the United States Congress has also done its part by actively participating in the approval of several legislation limiting China. The approval of the 2019 National Defense Authorization Act (NDAA2019) allowed the increase in the Department of Defense budget. The defense spending budget increases to meet the expenses involved in modernizing the US military and maintaining military preeminence and forward-based presence. The Department of Defense has shown special attention to the need to incorporate new technologies – "big data", artificial intelligence, quantum technology, 5G, and robotics to ensure the US military's technological advantage and compete with China.

Third, the issues addressed by the present administration are more varied and more politically sensitive, denouncing human rights violations within China, supporting the movement "Occupy Central" in Hong Kong (Jisi & Ran, 2019, p. 3), and expressing intentions for greater political participation in areas under political tension such as Taiwan and Tibet (Sutter, 2017, pp. 70-71).

As discussed above, relations between China and the US have shifted towards a more competitive relationship. At least two broad types of competitions appear to be taking place between the United States and China. First, the dispute is mainly about being first in emerging technologies with military use. The country that achieves the most militarily relevant innovations will be the one that obtains the largest benefits (Barnes & Chin, 2018). It is estimated that the new generation of technologies will ensure military superiority, information superiority, and economic superiority (Allen & Chan, 2017). Artificial intelligence has raised several alarms in matters of national security because on the battlefield, it provides speed and lethality. It also opens vulnerabilities to strategic nuclear stability (Fitzpatrick, 2019). Both countries have prioritized the development of AI technology. China has gone one step further, projecting that by 2030 to dominate the field of AI.

The Sino-American rivalry is not only commercial but also encompasses different dimensions. It should only be noted that after the tariff measures taken by the US in 2019, immediately after the attacks on Chinese technology companies began. The Trump administration prohibited US agencies from acquiring Huawei and ZTE equipment, and imposed greater restrictions on technology exports, put up stiff resistance to the adoption of Huawei's 5G technology at the same time that discouraged allies from allowing this technology into their countries. Allies, such as Australia, New Zealand, and Japan, followed the American instructions. In 2012, *US House Permanent Select Committee on Intelligence* report indicated Huawei as a company that represents a risk to the security of citizens because of dubious handling of information on devices and suspicions of a backdoor that allows them to collect information, functioning as a means of cyberespionage (Heinl, 2017, p. 140) and also a threat in the military sphere due to the company's relationship with the People's Liberation Army of China (PLA) (NO, 2017, p. 3). However, the accusations stated by the US have been rejected by Huawei company, and to add evidence to their statement, Huawei has allowed the equipment they produce to be examined by experts from Government Communications Headquarters (GCHQ) in search of malicious software or backdoors and so far they have not found anything wrong (Inkster, 2019, p. 109).

The international market positioning of Chinese companies is becoming more and more noticeable. Now more than ever before, China is competing more closely in the creation of advanced technologies, so one of the US priorities is to discourage the pace at which Beijing advances in technology development (Inkster, 2019, p. 109) for national security and commercial reasons (Lau, 2020, p. 22). The trade war is only one manifestation of the real competition in technology (Chen et al., 2019, p. 5; Lau, 2020, p. 19). The US attempts to counter China's efforts to become technological leadership and maintain its position as a dominant power by driving the world into a cold war over technology.

Second, a geopolitical rivalry for dominance in third states occurs on at least three dimensions: "maritime competition, competition for infrastructure funding, and competition for the digital network" (Mori, 2019, p. 81). To counter the "Made in China 2025" plan and China's "Belt and Road Initiative", the United States has pushed the "Free and Open Indo-

Pacific Strategy" (FOIP) (Jisi & Ran, 2019, p. 3). The strategy includes Australia, France, India, Indonesia, Japan, and the United States. The central idea is to transform the Indo-Pacific region into broader regional cooperation by thinking of the region as one maritime zone. Economic, military, maritime, and foreign policy aspects are discussed to achieve it (Scott, 2019). The United States has shared interests with Japan and Taiwan. Japan, which is at the juncture of deciding whether to counter or support China's rapid growth (Hosoya, 2019), and of course Taiwan, whose close relationship with the United States has raised concerns in mainland China (Auslin, 2018). However, both countries are experiencing a growing maritime pressure of The People's Republic of China (PRC) as a threat to their security (Scott, 2019, p. 49), and FOIP would help them decrease the tension with China by having the United States as an allied. The projects developed by China in recent years are interpreted as an indication that China is seeking greater global projection with geostrategic repercussions, for instance, the digital Silk Road (Vila Seoane, 2020), the Maritime Silk Road Initiative (MSRI), and the Silk Road Economic Belt (SREB) are projects with geopolitical impact (Blanchard & Flint, 2017). Jisi (2014) is of the opposite opinion. It considers a "march westwards" strategy, that is to say, the creation of multilateral relations with countries located in the west by China can benefit the relationship with the United States because it functions as a "rebalancing" that would avoid a confrontation at sea or on Chinese territory. In this sense, the mentioned proposals should not be interpreted as China's expanding global influence (Jisi, 2020) but rather as a "rebalancing" for more balanced Sino-US relations.

The US has a special interest in maintaining regional access to Asia to counteract China's influence. Its main strategy is to form strong alliances, such as the partnership with India (Parameswaran, 2018). However, the Trump administration has not been efficient in making allies; on the contrary, it repels them by initiating trade wars with partners and adversaries (Blankenship & Denison, 2019, pp. 51-52). In addition to the projects China is carrying out in the region and which, given their scope, extend beyond the region, it is gaining influence through economic and political involvement with different organizations such as the Association of Southeast Asian Nations (ASEAN) (Noguchi, 2011, p. 76). It also aspires to become a maritime power to "ensure access to energy resources, foreign trade, and direct investment, but also to guarantee its protection against possible external threats" (Noguchi, 2011, p. 66). The reaction of other nations to the Chinese nation with a greater global presence can impact their domestic development and their participation in the international sphere. However, the international community's correct interpretation of China's aspirations and values as it seeks its place in the international order will be important in shaping its relationship with the Western powers in the long run (Jisi, 2011).

There are at least three motives why Washington chose to follow a competition-based approach to China now and not before. First, the growing perception within the United States that a relationship based on engagement in the common interest has left them with few benefits, and conversely, China has taken advantage of this situation. As an example, the constant infringement of property rights and espionage for economic purposes. Second, the

American business community has expressed its discontent with the unfair competition they face within China and on US soil from Chinese competition. Third, the US sees the potential in China to interfere in domestic politics and influence societal opinion, including using devices to extract data from citizens (Mori, 2019, pp. 79-80).

The following sections outline how technological competition is developing in three ways: cyberspace, military technology, and artificial intelligence.

Cyberspace: A Battlefield for the US and China Rivalry

Cyberspace has become a contested domain, a critical battleground for the United States and China. In the last decade, the increase of cyber interactions in this domain provides us with enough information to analyze the motivation for competition between these two powerful states. As a matter of fact, both countries have ambitions for wide-ranging and rapid military modernization implementing new technologies and cyber capabilities. China has consistently focused on modernizing its military forces and developing military capabilities. Firstly, to maintain its regional dominance in the South China Sea, a region in constant dispute, and secondly to be able to cope with the US military power. Also, China competes for military dominance motivated by a desire for survival that goes beyond sovereignty and territorial integrity but is expressed in terms of keeping their resources and interests intact, so military competition is necessary for their survival.

Military superiority is one of the elements that have kept the United States as a hegemonic power. Therefore, China's actions have not gone unnoticed within the US defense and security community, and it has started to see a potential military rival in China, largely because there are many doubts regarding its capabilities and intentions. The motivations of both powers are leading us towards a direct military competition. The American government is motivated to be the leader in developing new and more sophisticated military technologies to maintain defensive military superiority but, above all, offensive to deter rivals while maintaining its global influence. For the United States, survival is one of the vital motivations to compete because within an anarchic international system, there are attempts to challenge its hegemonic role.

The PRC has begun to compete against the United States for military superiority, mostly through cyber capabilities for warfare in cyberspace (Domingo, 2016, pp. 157-158). China cannot compete with the US in conventional military force; the Lowy Institute Asia index 2018 shows the big difference in military capability among these great power; the United States score 94.6 out of 100, China 69.9, and in third place, Russia 61.4 (The Lowy Institute, 2018, pp. 5-11). China has a special interest in competing with the States in cyberspace because it takes advantage of the United States in this domain, dependence on the Internet to operate its critical national infrastructure, modest cyber defense, and weaknesses of US cyber-based systems. China is using the United States' cyber-dependency to its advantage.

Cyber dependence is a notion employed by Valeriano and Maness (2015), which measures the dependence of a state on the Internet to carry out its daily activities and the functioning of its infrastructure. Among the most cyber-dependent states in the world is Estonia in the first place, the United States, Germany in the same degree, and a little less China (Valeriano & Maness, 2015, pp. 25-26). The more cyber dependent a state is more cyber threat faces. Furthermore, cyber dependence associated with the "network readiness" notion, disclose why it is more important to control what happens in cyberspace for some state than for others. In this case, the US and China's network readiness are among the highest in the globe. This argument is well explained by Eriksson and Giacomello (2009, p. 209):

> *If the network readiness is low or insignificant, then, by all means, there is not much to control, and the dependency on information and communication technology (ICT) for the functioning of society and government is insignificant. If, however, network readiness is high or clearly growing, then the issue of Internet control is of much greater importance. It becomes more interesting to consider the various dimensions of control, especially such conditions as patterns of ownership and maintenance of critical infrastructure, governmental Internet policies (including censorship), dependency on multinational cyber-companies and other foreign interests, and the significance of global Internet governance initiatives.*

After a century of humiliation, China is beginning to revise the US-led international system, so Western interpretations of cyberspace and internet governance are being put on trial (Bey, 2018, p. 32). China is negotiating with the West international cyber rules that benefit its domestic policies (Bey, 2018, pp. 34-35) to ensure its national security, which depends largely on controlling the flow of information in cyberspace and Internet filtering. Jiang (2010) notes that Washington underestimates Beijing's capabilities to regulate the Internet. Consequently, there are an Internet Governance Wars (Franklin, 2009), between a single, connected internet promoted by the US. and a bordered internet endorsed by China, whose proposal is incompatible with the actual Internet governance regime; Internet Corporation for Assigned Names and Numbers (ICANN), the Working Group on Internet Governance (WGIG) and World Summits on the Information Society (WSIS) organizations dominated by public and private actors from the United States (Eriksson & Giacomello, 2009). American and Chinese ideas about the rules that should govern cyberspace are linked to the political positions they hold (Bey, 2018, p. 31). China is more emphatic in emphasizing the idea of cyberspace as a part of its territory over which it has sovereignty and does not allow it to function without its direct administration (NO, 2017, p. 4) and less allows the interference of external forces that impose rules on how the Internet should function within its border, cyberspace is inviolate and indivisible (Heinl, 2017, p. 136).

For the US, cyberspace represents a critical battleground because it allows competitors to operate continuously against them in search of strategic advantage and gain influence or control by breaking down networks and systems (Nakasone, 2019, pp. 13-14). The first initiative presented by the US government to counter the security challenges introduced by cyberspace is The Presidential Decision Directive 63 (PDD-63). It was developed in 1998 to protect the United States from the growing threats from cyberspace that can endanger national security. PDD-63 had a largely defensive emphasis, establishing the need to integrate computer network defense and computer network attack capabilities to maintain military dominance and address any threats from nations or non-state actors against American interests. More recently, in 2009, the United States Cyber Command was established. It is a joint command for offensive and defensive military operations in cyberspace (Sunday, 2016, p. 162).

Espionage in Cyberspace: An Old Conflict with a New Face

While state-sponsored cyber-attacks are accepted as a natural form of coexistence in cyberspace, industrial espionage and cyber-theft of intellectual property are being pointed out as the no-go line (Bey, 2018, p. 35) among great powers. China has been in an espionage dispute with the United States for over a decade (Akyesilmen, 2018, pp. 233-236). Valeriano and Maness (2015, p. 47) define cyberespionage as "the use of dangerous and offensive intelligence measures to steal, corrupt, or erase information in the Cyber-sphere of interactions". China is expertise exploiting gaps in America's cyberspace defenses; this tactic avoids direct confrontation in another realm of cyberspace. Espionage works as a low-level demonstration of a cyber capability. China has launched several cyber espionage campaigns against the US government and the private sector (Goodman, 2010). Unit 61398 and 61486 are two of the principal espionage groups which frequently targeting US political and military intelligence. Cyberespionage can be used long or short-term depending on the purpose. In the short-term, "consistent with covert actions, either gains access or merely sends an ambiguous signal of resolve altering short-term strategic calculus" (Valeriano et al., 2018). In the long-term, espionage seeks to manipulate the balance of information to accomplish a position of political, military, or economic advantage (Valeriano et al., 2018). China is most likely to engage in an espionage attack, both short and long-term. The US is most likely to engage in degradation operations. From 2000 to 2016, the US-Chinese dyad experience overall 48 Cyber conflicts, China 43 times initiated the incident and five by the US. The aim of China within these 48 interactions, 34, was short- and long-term espionage (Brandon & Maness, 2000-2016).

At present, for the US, the highest cost comes from intellectual property theft (IP theft) (Nye, 2017). According to Read (2014), the suitable concept for intellectual property theft performed online is economic cyberespionage, define as "the practice of infiltrating these networks to acquire a trade, technological or economic information to benefit a foreign country or foreign agent". Because the benefits far exceed the costs, China has no incentive to restrict its behavior (Nye, 2011). For example, in 2013, Chinese hackers exfiltrate data related to the C-17, a military transport aircraft, the C-17 research, and development cost $3.4 billion. Unquestionably, economic cyberespionage is cost-effective (Segal, 2016).

Read (2014) notes that after the 2010 Google's disclosure that China successfully infiltrated its network, the US government modified its position to the economic cyber-espionage threat. The attack on Google and at least 20 other companies is known as Operation Aurora and started in 2009. Until Operation Aurora, US politicians did not take proactive decisions to obstruct the economic cyber-espionage campaign. After Operation Aurora, the Obama administration showed significant attention to intellectual property management and economic cyberespionage. In the Sino-American relationship, these became dominant issues. In September 2015, President Obama threatened with economic sanctions against Chinese firms over state-sponsored cyber-attacks on American companies. The same year the two nations reached a bilateral agreement to halt cyberattacks used for economic espionage, which led to a decrease in this type of interaction. However, by 2018 China had started to enter the US networks again. In 2018, the United States launched The China Initiative to stop the theft of intellectual property by China and make it clear that these types of practices are not tolerated anymore (Healey, 2019). Nevertheless, to date, this remains an issue on which both nations have not reached a final agreement and remains a tense aspect of the bilateral relationship (Healey, 2019, pp. 143-144).

Intellectual Property (IP) theft can be of three types: patent theft, copyright theft, and trade secret theft. According to cyber studies literature, one of the main perpetrators of intellectual property theft is China. Trade secret theft, defense technologies, computer software, and source code are protected by US trade secret laws and are especially vulnerable to theft through hacking, international investment, or switching of companies from senior managers who take with them the knowledge to reproduce such technology (Healey, 2019, pp. 140-143). There are also American technology startups for which the Chinese market is too attractive, and the only way they are guaranteed market access is by offering to transfer technology to the Chinese government. Although American intellectual property laws protect the technology operated by these companies, American trade secrets are exposed through this legal mechanism imposed by the Chinese authorities on foreign companies. In this way, they manage to get hold of foreign technology (Healey, 2019, pp. 143-144). China's interest in accessing and developing new technologies through cyber-espionage threatens US economic competitiveness and has long-term costs to US innovation capacity (McRaven, 2019, p. 5) and defense capability.

China's use of cyber-attacks for industrial espionage is linked to its industrial policy. Together with several projects, cyberspace is aimed at making the country capable of producing high technology and designing its products and goods. AI technologies have received much attention from the Chinese government, and even though the United States leads this area, China is the fast-follower, allocating billions in investment and financing, since 2014 surpassed the United States in AI research and AI-related patent registration. Today is indisputable Chinese leadership in frontier technologies (McRaven, 2019, p. 40).

Nevertheless, US national security points out that the illicit behavior of the Chinese government is the means by which the government has achieved some technological advance and if in the future they manage to innovate, it will be the result of IP cyber theft and illegal technology transfer (Deutch, 2018, pp. 44-45).

China has no valuable reason to stop stealing intellectual property; on the contrary, the economic, technological, and military benefits deriving from this practice are far greater. Neither economic sanctions nor bilateral treaties have been able to eliminate this type of attack. The US cyber command has stated that the constant attack to which they are subjected in cyberspace requires them to fight and defend forward because their adversaries are engaged in offensive, defensive, and espionage operations, and these threats must not go unpunished (Healey, 2019, pp. 1-5).

The US cyber forces operate with a joint cyber strategy that combines cyber deterrence and active defense strategies; which consists of a constant presence in the cyberspace of the US cyber forces to be able to analyze the behavior of the enemy and "warn targets of the details of coming (or ongoing) attacks, improving US defense" and in the use of "cyber capabilities for deterrence purposes" (Healey, 2019, pp. 5). It should also be mentioned that the US cyber mission force has the power to carry out offensive operations, in the first instance to support "operational plans and contingency operations", and when the nation is the victim of a cyber-attack of significant proportions, it can carry out "action beyond blocking and after-action mitigation" (Kehler et al., 2017, p. 74). The 2015 *White Paper on Military Strategy* also made it clear that China's actions in cyberspace also contemplate active defense understood as "strategic defense and operational and tactical offense" (Kania, 2015) cyber-attacks are a means of reaction against any action that poses a threat (NO, 2017, p. 6). The force deployed in cyberspace is a sign of the increasing militarization that is taking place in this domain (Deibert, 2011).

The Militarization of Cyber Domain: Who Leads It?

The narrative of IP theft as a national security issue allows the United States to make two strategic moves; first, it allows it to point to states directly as being responsible for the theft of IP, for example, on the occasions that the United States has pointed out this practice, it directly blames China, rather than a group of hackers like The Red Hackers. Second, the division between "domestic economic innovation and the production of classified information" (Halbert, 2016, p. 256) becomes ambiguous as a consequence, the narrative of IP theft as a threat to national security is being used to validate the dominant presence of the United States in cyberspace, enhanced surveillance and control over the Internet for national security reasons.

Halbert (2016) identifies that it was in the document issued in 2008 entitled *Report to the 44th President of the United States on Cybersecurity* where the relationship between intellectual property and national security began to be shaped, and subsequent to this document is that the narrative began to be repeated in the following official documents issued by US presidents about the cyberspace (Halbert, 2016). In the May 2011 report *International Strategy for Cyberspace*, it states that to protect economic and national interests from threats such as IP theft, diplomacy will be used first but will also seek to deter and stop potential actors from threatening US national and economic security in cyberspace (Halbert, 2016, pp. 257-258). Intellectual property as a national security issue has "achieved a level of political valence akin to the elusive threat posed by the war on terror" (Halbert, 2016, p. 261) and open the possibility of military escalation (Halbert, 2016, p. 264). The increasing militarization of cyberspace and defensive actions of the US and China raise doubts about whether cyberespionage will continue to be interpreted as an unfriendly act or will have the impact of being considered an act of war.

On the other hand, there is reason to be concerned about the "danger discourse" around intellectual property theft that is being used in the first place to mobilize the military budget towards a strong cyber strategy which requires an accumulation of cyber resources and personnel to address the growing threats from the cyber domain, including intellectual property theft from state and non-state actors. Second, it is being used to monitor internet traffic, including a more in-depth analysis of civilian data.

At the end of the Pax Britannica, the United States took the place of global leader, which it has maintained mainly because of its scientific development, which has guaranteed economic and military supremacy over the other powers around the globe (Paarlberg, 2004). However, its technological leadership seems to be under threat. In 2004, Adam Segal wrote the essay *is America losing its edge?* and stated, "it would be premature to declare a crisis in the United States' scientific or technological competitiveness" (Segal, 2004). Sixteen years have passed since then, and the United States' situation is not the same. With its economic power, China mobilizes large investments towards the technological sector and rivals the United States in scientific or technological competitiveness (McRaven, 2019). China's intentions are not limited only to dominate labor-intensive manufacturing. The government is trying to develop China's indigenous technological capabilities to achieve military superiority, while the United States uses the arms embargo and tightened transfers on high technology, trying to constrain China's rise (Goldstein, 2015).

The technological development promoted by the Communist Party is recent compared to other industrialized countries. It started only 30 years ago. From 1950 to 1980, the government decided to open its market to foreign capital in exchange for technological transfer. In this period known as techno-nationalism, the manufacturing industry was primarily developed. In the 1990s, the government decided to make a strategic shift by emphasizing indigenous innovation because while neighboring countries like Korea and Japan produced high-end, high-tech products, China produced low-cost manufacturing products. By supporting enterprises through subsidies, free land, and low taxes, companies like Huawei could flourish. The government dramatically increased its participation in technological development and became the guide of a "national technological innovation" phase (Liu, 2016, pp. 4-5). It was also a strategy to counter the US embargo imposed in 1989. The embargo covers mainly US defense technology and military systems. Since 1990, the defense industry has been a priority for the Chinese Communist Party (Bräuner, 2013, pp. 557-558).

China has two purposes in enhancing its military power, in principle to weaken the US military advantages (Shifrinson, 2020, p. 197) in Asia-Pacific (Simón, 2020, pp. 5-6) following the philosophy of "win without fighting" and in the long run to catch up with the US and become a science and technology power (Kania, 2017, p. 5) to ensure military superiority in all domains. Friedberg (2018, p. 35) says that in Asia-Pacific, the US power projection system has been eroded by China's anti-access/area denial (A2/AD). In addition, he states that China is developing a naval strategy to project power beyond its shores, reaching out to "the Indian Ocean, the Persian Gulf and off the coast of Africa" (Friedberg, 2018, p. 38). As far as China is concerned, complemented and supported by other political instruments, the military instruments of the United States have two purposes: first, to enable the integration of Beijing into the processes of cooperative security and actions compatible with American interests in general. Second, to provide security to Asian allies by demonstrating that the United States has the military capability to provide security in the area and to discourage China from using military force as a means of conflict resolution in disputed areas, whether islands or states such as Taiwan (Swaine, 2011, pp. 147-148).

The ongoing military competition between the US and China is driven by two critical characteristics of the world technological scene. First, the commercial use and development of technologies such as artificial intelligence and quantum computing have increased. These technologies are both for military and civilian use making their proliferation and reflects greater diffusion than technologies exclusively for military use, resulting in state competitors and non-state actors being able to acquire them. Second, the first line of military competition is innovation because the development of high technology requires closing the gap between development and military implementation.

Washington and Beijing have responded to the changing innovation landscape. For its part, the United States has established Defense Innovation Unit Experimental (DIU) to get involved in the ecosystem of commercial, technological innovation. Chinese leaders have consolidated a civil-military fusion strategy that removes barriers between the private sector and the military-industrial base (Laskai, 2018a). China intends to transfer the success of the technology sector into military power. The civil-military fusion strategy allows it to involve the country's high-tech civilian companies in defense projects.

In May 2016, the Innovation-Driven Development Strategy (IDDS) was officially declared by Beijing. The focus of this strategy is China as a champion of innovation. It provides an insightful and forward-looking projection of China over the next three decades.

1. Becoming an "innovative country" by 2020
2. Joining the leading edge of advanced innovation countries by 2030
3. Becoming a strong global innovation power by 2050

In this regard, Xi Jinping has declared: "To carry out the innovation-driven strategy, the basic thing for us is to enhance our independent innovation ability…" (Xi, 2014, p. 134) because "Under a situation of increasingly fierce international military competition, only the innovators win" (Zhong, 2017). China has developed three projects in which it has set the course for the next decades to increase its technological capabilities. Integrated Circuit (IC) 2014 Guidelines aim to reduce the dependence on US integrated circuit manufacturing by developing a local industry that produces chips and meets the consumer needs of Chinese industries. Perhaps one of the most well-known projects is Made in China 2025, an ambitious project that aims to transform the manufacturing industry through three transitions "From China's speed to China's quality; from China's products to China's brands; and from 'made in China 'created by China" (Liu, 2016, p. 2). Implementing this strategy requires industries to modernize their factories to apply smart technologies and solve the challenges they face, such as labor costs, pollution, and delays in production and export. Next-Generation Artificial Intelligence (AI) Development Plan aims to make China a world leader in AI by 2030.

In addition to the civil-fusion strategy, in the behavior of the Chinese government, one can identify the development of the "Going Out" strategy that encourages technology transfer from overseas (Mori, 2019, p. 82). China is investing billions in new American companies with cutting-edge products that could have military applications. China's interest in US startups is focused on artificial intelligence and robotics. In this sense, the Trump Administration has made two important and necessary moves to define the future of the United States: reviewing carefully the process that allows Chinese investment in critical technologies and better controls on exports of sensitive technologies (Segal, 2019).

Artificial Intelligence Competition: A New Arms Race?

During the last decades, a technology that has burst onto the political scene is artificial intelligence (AI). Artificial intelligence can disrupt the international system (Demchak, 2019) and affecting the balance of power (Horowitz et al., 2018; Kania, 2017). Artificial intelligence can add sophistication, speed, precision, and lethality to military and strategic affairs (Payne, 2018). AI is a set of various computational techniques which operate in different dimensions, physically on objects: tanks, airplanes, robots can function without human intervention. In a non-tangible way, it operates in the processing and interpretation of information through image-recognition algorithms (Horowitz, 2018, p. 48). Also, AI is developed due to four analogous inputs "abundant data, hungry entrepreneurs, AI scientists, and AI-friendly policy environment" (Lee, 2018). These four inputs are found in large numbers in China.

We are entering into a phase where two great powers have an equal goal: to be the leader in all aspects of AI. Authors like Barnes and Chin (2018) estimate that this situation is triggering an escalating AI arms race because both nations want to be the first to find military applications of AI. Horowitz (2018) supports their point of view. He adds that there is a strong possibility that the use and development of autonomous lethal weapon systems will lead to an arms race. After all, military technology determines how wars will be fought and won (Sechser et al., 2019, p. 732).

The Pentagon has been closely following China's movements, especially those involving military investment. Since 2014, the United States has initiated efforts to become a leader in AI to increase and maintain its economic and military power. Barnes and Chin note that William Roper, then the head of the Pentagon's Strategic Capabilities, played a key role in getting the US government to take that direction and gain an advantage over China in the field of AI. However, in May 2017, a game between Ke Jie -the best player on earth of Go- against AlphaGo -one of the most advanced AIs in the world- triggered China to have its "Sputnik Moment". AlphaGo's victory from the Western viewpoint represented the victory of the machine over man. According to Lee for China, that game visualized in real-time by millions of Chinese affected the Chinese psyche and government policymakers, the West overwhelmingly showing its technological superiority and dominance in an era of artificial intelligence (Lee, 2018, pp. 11-29) which led the Chinese authorities to react.

Two months later of the Go game, China revealed to the world the *New Generation AI Development Plan 2017*, in it establishes its firm intentions to lead the world in AI by 2030, also sets out a three-dimensional agenda, namely "tackling key problems in research and development, pursuing a range of products and applications, and cultivating and expanding AI industry to 1 trillion RMB ($150 billion) by 2030" (Kania, 2017, p. 9). Since its release, China's national AI Plan has promoted AI as a high-level priority for Beijing. Military-Civil Fusion AI has made China emerge as an AI powerhouse by working as one team with companies such as Baidu, Alibaba, Tencent, and iFlytec (Horowitz et al., 2018, pp. 12-14).

Harnessing AI Technology, the Chinese Communist Party (CCP) intends to strengthen its national and military power (Ahmed et al., 2018). According to Barnes and Chin (2018), to overtake the United States in the field of AI, China has adopted the American strategy to use it against them, firstly the creation of a Chinese version of the Defense Advanced Research Projects Agency (DARPA) called The Scientific Research Steering Committee, which will report directly to President Xi Jinping and secondly investing heavily in Zhongguancun where China's Silicon Valley is located.

The first White House initiative in artificial intelligence was carried out in 2016 during the Obama administration's *National Artificial Intelligence Research and Development Strategic Plan*. However, it was not until February 11, 2019, that the United States presented a whole-of-government strategy called *AI Initiative*. The fact that it took three years to present an AI strategy has been criticized, pointing to the slowness with which the White House has pushed cutting-edge technologies (McRaven, 2019, pp. 47-48). Key principles stated in Obama's report were adopted more quickly in China than in the United States (Horowitz et al., 2018, p. 10). Dascalu (2018) compares the policies in AI presented by Obama and Trump concludes that: "the development of foreign AI policy will benefit the US as it will be a way to gain power through AI technologies and pursuing hegemony, as power will assure the survival of the US" (Dascalu, 2018, p. 35). In the last two years, the present administration has put considerable effort into prioritizing the development of artificial intelligence, a joint effort of both the White House and federal agencies to ensure that the US remains the world leader in AI. The most recent action by the White House was announced in February 2020. President's FY21 budget commits to double AI R&D over two years and the recent adoption of AI ethics principles by the Department of Defense.

In general, both countries have prioritized AI because of the economic advantages that can be obtained from creating AI for specific uses by having the advantage of being the first IP registrars to ensure economic leadership. And secondly, the military advantage over the opponents by applying AI capabilities to their military (Horowitz et al., 2018, pp. 11-12), such as automation of decision making, command and control, and autonomous systems. For China, artificial intelligence matters because it is crucial to the future global military and economic power competition, and also, achieving leadership in AI technology is a step towards reducing dependence on international technology imports (Allen, 2019, pp. 3-4). It is crucial for the US to achieve an offset strategy -first nuclear weapons, second stealth, and precision strike- and AI is announced in the US as the third offset strategy (Payne, 2018, p. 7).

Halbert (2016, p. 262) suggests that "the data theft undertaken by the Chinese is specifically designed to improve their military and technological capacities". However, having access to AI technology through cyber espionage or mimicry is not easy. Firstly, mimicking AI applications is expensive and complex. Governments that have developed this type of technology are forced to deal with the components in secrecy, which means that they are not found on the market mainly because they are classified. Also, the technical knowledge needed to develop, adapt, or modify algorithms and develop AI-based military capabilities requires advanced knowledge. Getting an AI application to work properly can take a long time. Secondly, the cybersecurity used by military technology to prevent hacking and spoofing is very high compared to the technology intended for civilian use, which adds an extra layer of security against copying attempts.

Is America Prepared for Winning the Competition Against China?

During the Cold War, the United States increased its power by engaging in internal and external balancing and overcoming the USSR. Since the end of the Cold War, the US has followed a strategy of primacy in different areas, domestic economic growth, technological innovation, and military might. However, nowadays, the US primacy seems to have ahead of the challenges that can take it to a level of competition similar to that of the Cold War. Blankenship and Denison (2019) question the capacity of the United States to successfully face this stage of the great-power competition against China because they perceive that the United States lacks internal and external balancing. Internal balancing is based on developing military and economic capabilities "and investing in technologies and other domestic areas that help convert the latent capabilities of the state into material strength" (Blankenship &

Denison, 2019, p. 45). In contrast, external balancing represents the creation and strengthening of strategic alliances to face a common threat. As long as the United States does not change its strategy in critical areas such as human capital, a better relationship with the private sector, and R&D expenditures, the risk of losing the present competition to China is real.

a) STEM Workforce

In the United States, the low number of American students graduating from sciences and engineering is becoming a critical weakness. On the other hand, in China, the number of students enrolled in graduate science, technology, engineering, and mathematics (STEM) education programs is three times higher than in the United States (Segal, 2019). Certainly, this trend will impact the labor market. Projections estimate that dependence on foreign STEM workers will increase significantly over the years (Deutch, 2018, p. 40). Another aspect that has received much attention is the large percentage of Chinese students participating in sensitive research fields. The US has pointed out that the Chinese government uses expatriates to access new technologies developed at universities and companies (McRaven, 2019, p. 51). China has also made great efforts to attract foreign talent, and even scientists in the US have been offered the opportunity to lead research projects in China (McRaven, 2019, p. 37).

b) Private Sector

Today, technological advances are more accelerated due to the growth of the business sector and the social demand for technological goods. Also, fundamental technologies for national security are linked to the private sector before the main actor was the state.

In the middle of technological competence, a natural ally for the United States should be the American technology community located in Silicon Valley (Segal, 2017). However, recent events show that the relationship is distant. For example, Google has refused to work with the DoD in Project Maven, which focuses on AI to enhance drone strikes in the battleground. Companies fear that by getting involved in projects of this nature, they will lose their market position. The government emphasizes national security issues while the private sector is more interested in profit and consumers. Clearly, both sectors have conflicting interests.

c) R&D

At the end of the Second World War, nations witnessed the benefits of technology for first movers. Radars, atomic bombs, and guided missiles result from US federal investment in universities, research, and science. However, at present, the United States has reduced investments in science, technology, and commercialization. American universities during the Cold War had been the cradle of innovation and strategic competition – now at a disadvantage against China's universities, which are investing more in higher education and R&D rather than cut funding (Kadtke & Wharton, 2018, pp. 4-5). The cause for the weakening of the R&D system in the US can be found at the state level. The shortage and cut funding have led universities to look for international students capable of paying high tuition fees to complete the budget that will allow universities to cover their regular expenses and scientific research (Blankenship & Denison, 2019, p. 49). If the trend continues, there is a possibility that in the coming years, emerging technologies will not be produced any less commercially by the U.S (Kadtke & Wharton, 2018, p. 3).

China's total R&D expenditure is increasing rapidly since 2008 but is still not catching up with the United States. Chinese R&D expenditures have been increasing considerably as their economy grew, and a greater percentage of GDP has been allocated to this area, with a target of 2.5% of GDP. If China continues with this trend, it is estimated that by 2030 it will surpass the United States in R&D expenditures (McRaven, 2019, p. 37). As a result of increased investment in R&D and STEM worker advantage, "China is closing the technological gap with the United States" (McRaven, 2019, p. 39). Since 2016 China leads the world in scientific paper production and has a greater impact than a paper written by Americans because Chinese's paper has "clear technological applications" (McRaven, 2019, p. 40).

Concluding Remarks

Great power competition is a fact in the history of international relations. This competition takes place with the tools and instruments of the time. As the fifth domain of warfare (Clarke & Knake, 2019), cyberspace plays a battlefield for US-China power politics. As a revisionist and emerging cyber power, China has been challenging US hegemony in the last two decades. It has been investing in cyber technology for a long time and using the technology very effectively in many areas, such as AI, cyber intelligence, and the military. The question is: has China a chance to win this conflict?

Despite the advances China is making, there are doubts that it can surpass the United States in emerging technologies such as AI, genetics, or robotics. Technological innovation is closely related to the infrastructure that drives innovation; university-industry cooperation, intellectual property, publications, patents, research and development taxes, technology transfer, access to capital, and investment (Deutch, 2018, p. 42). In this sense, China's innovation infrastructure is taking its first steps, while in the United States, it is strong and mature.

China's actions, such as technology transfer and intellectual property theft, cyber espionage, have repeatedly been considered a threat to US innovation and technological leadership. Copying was once a viable option for those trying to access technological advances (Paarlberg, 2004, p. 141). However, the new wave of emerging technologies requires the dominance of knowledge because the complexity of the technology is greater, making it more difficult to imitate. According to Gilli & Gilli, China's use of cyberespionage is doomed to failure because it is impossible through imitation to close the military-technological gap with the United States (A. Gilli & M. Gilli, 2019, pp. 178-187). On the other side, the tacit knowledge of the US and the organization's know-how could maintain its military technological superiority unrivaled (A. Gilli & M. Gilli, 2019, pp. 187-188).

Another American advantage is its decentralized state structure. While centralization facilitates policy formulation, a decentralized state has greater advantages in promoting innovation and maintaining the technological edge (Drezner, 2001). The Military-Fusion strategy manifests the idea of cohesion between the private sector and the CCP, but the relationship has frictions. The success of the technology sector has not yet been reflected in significant technological advantages (Laskai, 2018a). Beijing has more facilities for the policy-making process but more difficulties in making it work. Also, Kennedy (2016) mentions that one of the policy challenges that China has to face is the constant government monitoring in the management of research and development, which is detrimental to the innovation process.

References:

Ahmed, S., Bajema, N. E., Bendett, S., Chang, B.A., Creemers, R., Demchak, C. C., Denton, S. W., Ding, J., Hoffman, S., and Joseph, R. (2018). *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives.* https://apps.dtic.mil/dtic/tr/ fulltext/u2/1066673.pdf

Akyeşilmen, N. (2018). *Disiplinlerrarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik. Ankara: orion Kitabevi.*

Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Belfer Center for Science and International Affairs Cambridge. https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

Allen, G.C. (2019). *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security*. Center for a New American Security. https://nsiteam.com/social/wp-content/uploads/2019/05/CNAS-Understanding-Chinas-AI-Strategy-Gregory-C.-Allen-FINAL-2.15.19.pdf

Auslin, M.R. (2018). *The Question of American Strategy in the Indo-Pacific.* A Hoover Institution Essay on a US Strategic Vision in a Changing World.

Barnes, J.E., & Chin, J. (2018). The new arms race in AI. *The Wall Street Journal, 2.*

Bernstein, R., & Munro, R.H. (1997). The coming conflict with America. *Foreign Affairs*, 18-32.

Bey, M. (2018). Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition. *The Cyber Defense Review*, *3*(3), 31-36.

Blanchard, J.-M. F., & Flint, C. (2017). The Geopolitics of China's Maritime Silk Road Initiative. *GEOPOLITICS*, *22*(2), 223-245.

Blankenship, B.D., & Denison, B. (2019). Is America Prepared for Great-power Competition? *Survival*, *61*(5), 43-64.

Brandon, V., & Maness, R.C. (2000-2016). *Dyadic Cyber Incident Dataset* (Version 1.5). http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/ dcid_version_1.5_public_final.xlsx

Bräuner, O. (2013). Beyond the Arms Embargo: EU Transfers of Defense and Dual-Use Technologies to China. *Journal of East Asian Studies*, *13*(3), 457-482.

Chen, A.W., Chen, J., & Dondeti, V.R. (2020). The US-China trade war: dominance of trade or technology? *Applied Economics Letters*, *27*(11), 904-909.

Cheung, T.M., Mahnken, T., Seligsohn, D., Pollpeter, K., Anderson, E., and Yang, F. (2016). Planning for innovation: Understanding China's plans for technological, energy, industrial, and defense development. *Report prepared for the US-China Economic and Security Review Commission, 155*.

Copeland, D.C. (2012). Realism and neorealism in the study of regional conflict. *International relations theory and regional transformation*, 49-73.

Dascalu, F.G. (2018). *In the Interest of the Nation: A Case Study of Artificial Intelligence Policy in the United States*.

Demchak, C. C. (2019). China: Determined to dominate cyberspace and AI. *Bulletin of the Atomic Scientists*, *75*(3), 99-104.

Deutch, J. (2018). Is Innovation China's New Great Leap Forward? *Issues in Science and Technology*, *34*(4), 37-47.

Domingo, F.C. (2016). Conquering a new domain: Explaining great power competition in cyberspace. *Comparative Strategy*, *35*(2), 154-168.

Drezner, D. (2001). State structure, technological leadership and the maintenance of hegemony. *Review of International Studies*, *27*(1), 003-025.

Erickson, A., & Goldstein, L. (2006). Hoping for the Best, preparing for the worst: China's response to US hegemony. *Journal of Strategic Studies*, *29*(6), 955-986.

Eriksson, J., & Giacomello, G. (2009). Who controls the Internet? Beyond the obstinacy or obsolescence of the state. *International Studies Review*, *11*(1), 205-230.

Fitzpatrick, M. (2019). Artificial Intelligence and Nuclear Command and Control. *Survival*, *61*(3), 81-92.

Franklin, M. (2009). Who's who in the 'internet governance wars': hail the phantom menace? *International Studies Review*, *11*(1), 221-226.

Friedberg, A.L. (2015). The debate over US China strategy. *Survival*, *57*(3), 89-110.

Friedberg, A.L. (2018). Competing with China. *Survival*, *60*(3), 7-64.

Gilli, A., & Gilli, M. (2019). Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security*, *43*(3), 141-189.

Gilpin, R. (1988). The theory of hegemonic war. *The Journal of Interdisciplinary History*, *18*(4), 591-613.

Goldstein, L.J. (2015). *Meeting China halfway: How to defuse the emerging US-China rivalry*. Georgetown University Press.

Goodman, W. (2010). Cyber deterrence: Tougher in theory than in practice? *Strategic Studies Quarterly*, *4*(3), 102-135.

Grieco, K.A. (2018). The 2018 national defense strategy: continuity and competition. *Strategic Studies Quarterly*, *12*(2), 3-8.

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, *5*(1).

Hoadley, D.S., & Lucas, N.J. (2018). *Artificial intelligence and national security*. Congressional Research Service.

Horowitz, M., Allen, G., Kania, E., and Scharre, P. (2018). Strategic Competition in an Era of Artificial Intelligence. *Center for New American Security (Washington, DC: Center for New American Security, 2018), 8*.

Horowitz, M.C. (2018). Artificial Intelligence, International Competition, and the Balance of Power. *Texas*

National Security Review, 37-57. https://repositories.lib.utexas.edu/bitstream/handle/2152/65638/TNSR-Vol-1-Iss-3_Horowitz.pdf?sequence=2

Hosoya, Y. (2019). FOIP 2.0: The Evolution of Japan's Free and Open Indo-Pacific Strategy. *Asia-Pacific Review*, *26*(1), 18-28.

Jiang, M. (2010). Authoritarian informationalism: China's approach to Internet sovereignty. *SAIS Review of International Affairs*, *30*(2), 71-89.

Jisi, W. (2011). China's search for a grand strategy: A rising great power finds its way. *Foreign Affairs*, 68-79.

Jisi, W. (2014). Marching Westwards: The Rebalancing of China's Geostrategy. In S. Binhong (Ed.), *The World in 2020 According to China* (pp. 129-136). Brill.

Jisi, W. (2020). Assessing the radical transformation of US policy toward China. *China International Strategy Review*, 1-10.

Jisi, W., & Ran, H. (2019). From cooperative partnership to strategic competition: a review of China–US relations 2009–2019. *China International Strategy Review*, *1*(1), 1-10.

Johnson, J. (2019a). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, *35*(2), 147-169.

Johnson, J. (2019b). The end of military-techno Pax Americana? Washington's strategic responses to Chinese AI-enabled military technology. *The Pacific Review*, 1-28.

Kadtke, J., & Wharton, J. (2018). *Technology and National Security: The United States at a Critical Crossroads*. Government Printing Office.

Kania, E.B. (2017). *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*. Center for a New American Security. https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinasfuture-military-power

Kennedy, A.B. (2016). Slouching tiger, roaring dragon: comparing India and China as late innovators. *Review of International Political Economy*, *23*(1), 65-92.

Kennedy, A.B., & Lim, D.J. (2018). The innovation imperative: technology and US–China rivalry in the twenty-first century. *International Affairs*, *94*(3), 553-572.

Laskai, L. (2018a). Civil-military fusion: The missing link between China's technological and military rise. *Council of Foreign Relations*. https://www.cfr.org/blog/civil-military-fusion-missing-link-between-chinas-technological-and-military-rise

Laskai, L. (2018b). Why does everyone hate made in China 2025? *Council on Foreign Relations, March*, *28*.

Lau, L.J. (2020). Economic relations between China and the US *Journal of Chinese Economic and Business Studies*, 1-37. https://doi.org/10.1080/14765284.2020.1712887

Layne, C. (2012). This time it's real: the end of unipolarity and the Pax Americana. *International Studies Quarterly*, *56*(1), 203-213.

Lee, K.-F. (2018). *AI superpowers: China, Silicon Valley, and the new world order*. Houghton Mifflin Harcourt.

Lin, Y. (2020). 'Made in China 2025'and China's cross-border strategic M&As in OECD countries. *Journal of Chinese Economic and Business Studies*, 1-24.

Liu, S.X. (2016). Innovation design: made in China 2025. *Design Management Review*, *27*(1), 52-58.

Mattis, J. (2018). *Summary of the 2018 national defense strategy of the United States of America*. https://apps.dtic.mil/dtic/tr/fulltext/u2/1045785.pdf [Access date: 21.01.2020].

McRaven, J.M. a. W.H. (2019). *Innovation and National Security Keeping Our Edge*. https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf

Mori, S. (2018). US Defense Innovation and Artificial Intelligence. *Asia-Pacific Review*, *25*(2), 16-44.

Mori, S. (2019). US Technological Competition with China: The Military, Industrial and Digital Network Dimensions. *Asia-Pacific Review*, *26*(1), 77-120.

Noguchi, K. (2011). Bringing Realism Back In: Explaining China's Strategic Behavior in the Asia-Pacific. *Asia-Pacific Review*, *18*(2), 60-85.

Nye, J. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44-71. https://doi.org/10.1162/ISEC_a_00266

Nye, J.S. (2011). *The Future of Power*. Public Affairs.

Nyrén, P. (2019). *China's Liberal Hawk: Yan Xuetong's Vision for Chinese Benevolent Dominance*. https://thediplomat.com/2019/06/chinas-liberal-hawk-yan-xuetongs-vision-for-chinese-benev

Paarlberg, R.L. (2004). Knowledge as power: science, military dominance, and US security. *International Security*, *29*(1), 122-151.

Parameswaran, P. (2018). ASEAN's Role in a US Indo-Pacific Strategy. *Woodrow Wilson International Center for Scholars, Asia Program*.

Paul, E. (2020). Techno-nationalism in China–US Relations: Implications for Universities. *East Asian Policy*, *12*(02), 80-92.

Payne, K. (2018). Artificial Intelligence: A Revolution in Strategic Affairs? *Survival*, *60*(5), 7-32.

Rasser, M. (2020). *Countering China's Technonationalism*. The Diplomat. https://thediplomat.com/2020/04/countering-chinas-technonationalism/

Read, O. (2014). How the 2010 attack on Google changed the US government's threat perception of economic cyber espionage. In *Cyberspace and international relations* (pp. 203-230). Springer.

Reuveny, R., & Thompson, W.R. (2001). Leading sectors, lead economies, and economic growth. *Review of International Political Economy*, *8*(4), 689-719.

Saunders, P.C., & Bowie, J.G. (2016). US–China military relations: competition and cooperation. *Journal of Strategic Studies*, *39*(5-6), 662-684.

Scott, D. (2019). Taiwan's Pivot to the Indo-Pacific. *Asia-Pacific Review*, *26*(1), 29-57.

Sechser, T.S., Narang, N., & Talmadge, C. (2019). Emerging technologies and strategic stability in peacetime, crisis, and war. *Journal of Strategic Studies*, *42*(6), 727-735.

Segal, A. (2004). Is America Losing Its Edge-Innovation in a Globalized World. *Foreign Aff.*, *83*, 2.

Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. Hachette UK.

Segal, W.M.J.M.A. (2019, November 18). America faces fresh challenges to technology innovation leadership. *The Hill*. https://thehill.com/opinion/technology/461958-america-faces-fresh-challenges-to-technology-innovation-leadership

Shifrinson, J. (2020). The rise of China, balance of power theory and US national security: Reasons for optimism? *Journal of Strategic Studies*, *43*(2), 175-216.

Simón, L. (2020). Between punishment and denial: Uncertainty, flexibility, and US military strategy toward China. *Contemporary Security Policy*, 1-24.

Sutter, R. (2017). Barack Obama, Xi Jinping and Donald Trump—Pragmatism Fails as US-China Differences Rise in Prominence. *American Journal of Chinese Studies*, 69-85.

Swaine, M.D. (2011). *America's challenge: engaging a rising China in the twenty-first century*. Carnegie Endowment.

Swaine, M.D. (2018). Chinese views on the US national security and national defense strategies. *China Leadership Monitor, 56*, 1-15.

The Lowy Institute. (2018). *The Lowy Institute Asia Power Index*. T. L. Institute. https://power.lowyinstitute.org/downloads/LowyInstitute_AsiaPowerIndex_2018-Summary_Report.pdf

Trump, D.J. (2017). *National security strategy of the United States of America*. https://apps.dtic.mil/dtic/tr/fulltext/u2/1043812.pdf

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

Valeriano, B., & Maness, R.C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.

Vila Seoane, M.F. (2020). Alibaba's discourse for the digital Silk Road: the electronic World Trade Platform and 'inclusive globalization'. *Chinese Journal of Communication*, *13*(1), 68-83.

Xi, J. (2014). *The governance of China*. Foreign Languages Press.

Xuetong, Y. (2019). *Leadership and the rise of great powers*. Princeton University Press.

Zhao, M. (2019). Is a new Cold War inevitable? Chinese perspectives on US–China strategic competition. *The Chinese Journal of International Politics*, *12*(3), 371-394.

Zhong, T. (2017). *'Scientific and Technological Innovation, Towards a Powerful Engine for the World-Class Military' ['科技创新，迈向世界一流军队的强大引擎'].* http://www.gov.cn/xinwen/2017-09/15/content_5225216.htm