SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 6732-6742
Open Access. Online & Print

DOI: 10.5281/zenodo.12426693

EMPLOYING CYBERSPACE IN COMPETITION AND THE STRUGGLE FOR DOMINANCE OVER CYBER TECHNOLOGY

Huda Khalaf Ali Ahmed[1]*, Prof. Dr. Hala Khalid Hamid[2]

[1]Republic of Iraq, Ministry of Higher Education and Scientific Research, University of Baghdad – College of Political Science, Department of International Studies
Email: huda.ali2201@copolicy.uobaghdad.edu.iq
[2]Republic of Iraq, Ministry of Higher Education and Scientific Research, University of Baghdad – College of Political Science, Department of International Studies
Email: dr.halakh@copolicy.uobaghdad.edu.iq

Received: 29/12/2025
Accepted: 20/02/2026

Corresponding Author: Huda Khalaf Ali Ahmed (huda.ali2201@copolicy.uobaghdad.edu.iq)

ABSTRACT

The world today can now see a great rise in technological competition amongst the nations especially between United States and China. This rivalry has not only assumed economic aspects but also has strategic and security aspects. This competition is a significant example of the opposition between commercial enterprises, and in particular, Huawei, because the rivalry between technological companies has developed into the sphere of influence, control, and tools of international power. The advent of the fifth-generation (5G) technology and the Huawei crisis brought about a lot of controversy in the world following the addition of the company to the blacklist of the United States and claims of intellectual property theft and espionage. Such steps resulted in the limitation of American businesses, which did not allow them to interact with Huawei and deprived it of such a significant technology as Android and semiconductors. On the side of china, these were seen as an effort to cripple it in terms of the 5G network development in the context of Made in China 2025 strategy. These dangers of this war have presented themselves in the areas of security, technology, and economy, especially after the arrest of Meng Wanzhou in Canada in 2018 that transformed the case into a symbol of technological and geopolitical rivalry of the two giants.

KEYWORDS: Cyberspace, U.S.–China Rivalry, Technological Competition, 5G Networks, Huawei, National Security, Made in China 2025.

Section One: U.S.–China Competition for Control of Cyberspace

Ever since Hu Jintao, the previous president of China stated in 2007, during the 17 th National Congress of the Chinese Communist Party, that China must invest in its soft power along with its military and financial prowess, China has implemented holistic approaches to increase its influence politically and culturally in the global scene. Hu Jintao stressed that when a country uses only military and economic force, it might become a point of concern among other nations and evoke them into devising counter-alliances, but with the help of soft and hard power, China will be perceived as a pleasant and appealing force, which will decrease the chances of the collective opposition. The Chinese model has found its way in the giant investments in high profile projects like Beijing Olympics, Shanghai Expo and the worldwide spread of Confucius Institutions. However, in spite of worldwide attention to GDP and economic factors of China, the United States is much and much ahead when it comes to military forces. China is doubtful of being able to match up in this field in the next decade.

Despite the inner limitations to civil society, China still desires the reinforcement of its soft power since the formation of political and cultural power heavily relies on non-governmental efforts of society. It is well-evidenced in the case of the American experience as soft power has been obtained through non-governmental organizations, including Hollywood, the Bill and Melinda Gates Foundation, and Harvard University. Joseph Nye, in this regard, counseled a Chinese student that China must relax internal censorship to build up its soft power by using the example of Bollywood, where the private sector is free to produce huge cultural impact despite the limits, which are in place.

After the Chinese government proclaimed two strategic Centenary Goals, which form one of the cardinal points of the modern technological and developmental path of China, the first goal was proclaimed in 2010, and was to increase per capita income and GDP by 2021, the same year the Chinese Communist Party will be marking its centenerary. The second goal is for China, by 2049 the centenary of the founding of the People's Republic of China to become a developed, strong, prosperous, and harmonious democratic state. It appears that China has made steady progress toward achieving the first goal, with its GDP growing annually at an average rate of 7.4% between 2010 and 2018. Additionally, China implemented an ambitious plan to eliminate poverty by 2020. Despite these achievements, the second centenary goal remains somewhat ambiguous. Nevertheless, since 1978, China has transformed from one of the poorest economies in the world into a middle-income economy, with per capita income rising from approximately $200 to nearly $10,000 by 2018. In contrast, it is projected that by 2049, per capita income in the United States may range from one-quarter to two-thirds of that in the People's Republic of China. The primary driver of China’s rise has been economic reform, particularly the transition from a centrally planned economy to a market-oriented economy. The 2008 Global Financial Crisis marked a pivotal moment in China’s development experience, as its economy managed to maintain stability and growth despite some structural imbalances. (Dollar, 2020)

As a result, American concerns have intensified over the growing Chinese influence in the technological domain, which is perceived as a potential threat to U.S. economic and military superiority. During his first term, Donald Trump, within the framework of his protectionist policies, sought to impose restrictions on companies with more than a 25% Chinese ownership stake when attempting to acquire American technology or invest in U.S. sectors related to national security, such as artificial intelligence, microchips, robotics, and encryption. It is expected that the expansion of China’s technological capabilities, particularly in the field of artificial intelligence, will further escalate tensions between the two countries, given its wide-ranging applications in both civilian and military domains. In addition, the United States Department of Defense called for increased government spending to counter China’s rising ambitions in artificial intelligence. (Khalifa, 2025). The U.S. government also urged stronger cooperation and coordination with American technology companies. (Al-Masawi, 2021). Furthermore, the United States has declared that China seeks to obtain sensitive technologies and intellectual property rights to enhance its military capabilities, posing a threat to American security and economic interests. It has also been suggested that some Chinese researchers and students, at institutions such as University of Oxford and other universities, could be exploited to gather such information, particularly if they are linked to the Chinese military. (Proclamation, No.10043)

Accordingly, and based on the powers granted to the U.S. president under immigration laws, entry restrictions were imposed on such students and

researchers, with limited exceptions for undergraduate students or those not associated with China's civil-military integration strategy.

These are measures that will help protect the U.S. interests and avoid misuse of scientific research by the military. The U.S. economy and national security on the other hand have become overly and even totally reliant on information technology and digital infrastructure that have penetrated into critical sectors of economy and business including energy, banking, telecommunications, transportation, the military industry, finance, healthcare, agriculture, water resources, logistics, emergency services, postal systems, and chemicals. With this interdependent relationship in the technologies and economic sphere, the cyber relationship between the United States and China has become very tricky. (Creden, 2017))

Although concerns about cybersecurity problems were mutual between the two countries in recent years, there are still considerable problems with establishing effective collaboration or understanding between the two countries. The relationship between them has been slowly developing into the state of almost total mistrust related to motives, interests, and actions, which has affected other spheres of bilateral relations adversely. Therefore, the foreign policy and actions of China on cyberspace are based on one major goal, which is the safeguarding of the ruling Chinese Communist Party and its further grip on power.

The authors Bo Singer and Allan Friedman argue that since the United States assumes that the Chinese government exercises extensive control over its domestic networks and citizens, it is natural for it to conclude that China is behind most of the malicious cyber activities originating from within its territory. Based on this assumption, the United States formally accused the People's Republic of China of responsibility for cyberattacks targeting the email servers of Microsoft Exchange. In this regard, the United States Department of State issued a statement declaring: *"The United States holds the People's Republic of China accountable for a pattern of irresponsible and destabilizing behavior in cyberspace that poses a serious threat to our economic and national security."* The statement further added that *"responsible states do not recklessly endanger the security of global networks, nor do they provide safe haven for cybercriminals or knowingly cooperate with them."* It also noted that hackers affiliated with the Chinese government have caused significant financial losses to governments and companies through ransom payments, intellectual property theft, and the destabilization of cybersecurity, while China's Ministry of State Security allegedly incorporated such hackers into its official payroll. Moreover, the The New York Times reported that Chinese technology companies have recently begun publishing job advertisements seeking Cambodian-language speakers, an unusual development, offering monthly salaries ranging from $1,200 to $3,000, ostensibly for research-related work.(ElSiyasa News.2025)

The Chinese president, Xi Jinping, has also announced plans to transform China into a "cyber superpower," emphasizing the importance of "cyber sovereignty" as the right of every state to determine its own path in cyber development, public policies governing cyberspace, and the regulation of internet content, in a manner that ensures equality with other states.(Schia and Gjesvik, 2017)

In February 2014, Chinese leaders introduced the concept of a "cyber superpower" (sometimes translated as a "network power"), making it a cornerstone of national strategy after Xi Jinping assumed leadership over the country's top cyber governance body. This concept is regarded as a critical element for achieving the goals of the Chinese Communist Party in its centenary and for securing a prominent global position for the People's Republic of China by 2049. Since then, the concept has become widespread in official discourse and serves as a guiding framework for China's national strategy in information and communication technologies. In 2015, during the World Internet Conference, Chinese leaders announced their intention to implement a strict and robust strategy aimed at building a "community with a shared future in cyberspace," as reflected in official statements since 2014.(Doutchi et al, 2021)

China has also issued policies asserting that internet traffic entering its territory must be subject to its sovereignty. Meanwhile, the United Nations General Assembly acknowledged in 2013 the importance of respecting states' cyber sovereignty. In 2015, as part of strengthening its offensive and defensive capabilities, China established the People's Liberation Army Strategic Support Force within the restructuring of the People's Liberation Army.

Operational duties such as satellite launching, cyber warfare, intelligence and surveillance, and network systems management are operational responsibilities of this force and the indication of an evident change in military priorities, which is the integration of cyber capabilities in the military

actions and the main focus on strategic deterrence to ensure the security of the Chinese interests both locally and internationally.

The new challenges revolve around the risk management by evaluating the origin of threats, properly determining the origin of cyberattacks, identifying the targeted vulnerabilities, and assessing the overall effects of the cyberattacks. Effective cyberattacks have the potential to have a tremendous impact on the national security, stability, critical infrastructure, and the safety of the citizens.

According to China, cyber sovereignty goes beyond cybersecurity, but it must also be understood as the utilization of any information to manipulate and shape the decision-making process of the adversaries. This strategy is based on technology self-sufficiency. As such, in 2016, China introduced a five-year plan worth a sum of 233 billion dollars and was the first nation to embrace the idea of the so-called sovereign internet, as well as the practices of ensuring information exchange, surveillance, and blocking access to other websites. These initiatives are taking place in the context of larger issues that are associated with the effort to identify cyberspace as a state domain, control it, delimit it, and develop a moderate response to national security challenges (Farahat, 2020).

In response to these risks, China established specialized civilian and military units dedicated to cyber warfare. (Al-Bahi, 2020). It has maintained its sovereignty by blocking and monitoring software and websites deemed threatening, setting global standards to limit backdoors and protect data, and developing advanced cyber capabilities, including both civilian and military hacker units.

With the growing importance of cyberspace, digital sovereignty has come to be regarded as the fourth domain after land, air, and sea, necessitating the protection of digital borders against what is described as "digital occupation." (Al-Dalil, 2021). On the global level, China considers its alliance with Russia a strategic step, as Russia represents a nuclear power capable of confronting the United States.(Segal, 2020)

To support its positions in international affairs, China together with Russia has worked to strengthen political and military cooperation, formulate joint policies, reshape the global cyberspace order, promote the concept of cyber sovereignty, and reinforce domestic control. These efforts aim to counter U.S. influence and respond to the U.S. National Cybersecurity Initiative, which focused on protecting cyber systems and enhancing both offensive and defensive capabilities.(Otkin, 2003)

China has also achieved significant progress in the production of capital goods and advanced technologies, with these products accounting for approximately 25% of its exports. Chinese manufacturers and companies dominate between 50% and 75% of the global market in power generation equipment and shipping containers. They also control around 30% of the global market for high-speed rail systems and telecommunications equipment. China relies on the Belt and Road Initiative to expand its economic influence across Eurasia, allocating an estimated budget of about $1 trillion. This provides Chinese companies with a substantial competitive advantage beyond their borders. Moreover, China derives significant military, economic, scientific, and cultural benefits from its space program, particularly through remote sensing technologies, which enable forest monitoring, agricultural productivity enhancement, desertification tracking, and water resource management. Chinese satellites also support space broadcasting and enhance telecommunications, serving both political and cultural objectives.

China rests great significance on space sciences through specialized centers and institutes, uniquely the China Academy of Space Technology, which is responsible for developing and manufacturing satellite components. China is striving to achieve technological self-sufficiency in these sensitive industries in order to compete with major powers such as the United States and Japan. (Arjoun, 1996). Although both the United States and China have at times attempted to ease diplomatic tensions, confrontations between them have resurfaced, often accompanied by reciprocal cyberattacks. Despite receiving extensive global media coverage, these incidents have not resulted in formal legal actions.

According to Jamie Metzl (the Executive Vice President of the Asia Society and a former official at the U.S. National Security Council, the U.S. Department of State, and the Senate Foreign Relations Committee), and based on official reports, China is considered one of the leading countries involved in cyber espionage and cyber hacking. This was also confirmed by the Pentagon in 2010, which indicated that China has been developing its cyber capabilities to target strategic information. Additionally, the U.S.-China Economic and Security Review Commission reported that the Chinese Communist Party and the Chinese government conduct cyberattacks against American systems and institutions. Other reports have further suggested

that China engages in commercial espionage as a strategic tool to enhance its military and economic superiority.

In 2015 China formed the People peacemaking Liberated Army Strategy help force as a segment of extensive military reforms to improve its capacities in the cyber sphere and include them into military service. This force is deemed to be one of the most important tools of strategic deterrence, as it will help the military to work successfully in the information warfare, protecting the global interests of China. It is formed of special components which are in charge of cyber warfare management, launching and operation of satellites, communications, and reconnaissance and survey though it is not a sovereign command like its counterparts in the United States.

China is also considered as one of the first nations to form a dedicated cyber warfare unit which is concerned with the development of electromagnetic pulse (EMP) weapons. These arms are similar to gamma pulse radiations produced by nuclear explosions that are capable of paralyzing computers and other electronics. These weapons are gained to be developed as a project named the Assassin Mace, and China is secretly developing these abilities through the use of state-of-the-art technologies. The discussion of integration of Taiwan after the reintegration of Hong Kong and Macau still continues in China. (Hunington, 1996). Meanwhile, it has intensely boosted its military budget, which was 119 billion 2011 to 248 billion in 2018. (Al-Anbari, 2022)

These developments have left the United States alarmed even though China denies that it is in an arms race as this has seen it label the civil-military integration in China as a security threat. This integration has been integrated by Xi Jinping in his 2016 reform agenda and a commission to create dual-use technologies has been formed thus enhancing the capabilities of the People's Liberation Army. The United States has been shifting to more severe actions in response to the rising number of cyberattacks by the Chinese, following the evidence that units of the People's Liberation Army were involved in extensive levels of hacking and espionage of American institutions and companies .

Advanced Chinese cyberattacks have been a challenge to the United States that has developed over decades and is now more sophisticated, stealthy, and difficult to track. (Albaslah.com, 2025). Based on the failure to protect sensitive information, experts have confirmed that the Chinese intrusion of the Office of Personnel Management in 2014 was catastrophic, and people were critical of the circumstances. (Skynewsarabia, 2025). In that regard, Michael Hayden, the former head of the National Security Agency, said: not shame on China, but shame on us, that we did not adequately secure this type of information. (Brands, 2020)

The United States is regarded as having one of the main adversaries in China both in conventional military and cyber space. It has explicitly shown desire of economic and military dominance and it has been utilizing the cyberspace as one avenue of realizing these objectives. The Chinese hackers have engaged in systematic cyberattacks on European and American industrial companies between 2010 and 2015 to steal data pertaining to the manufacturing of both military and commercial aircraft. This data was subsequently applied to create Chinese commercial aircrafts (Albrecht, 2021)

Alarm has been raised in the West and the United States over the capabilities of China in cyber activities, against the background of allegations that the Chinese government is sponsoring recurrent cyberattacks into large American institutions, companies, and universities. In this regard, the Center of a New American Security released an article, called The Combatant State, where the authors investigated the cybersecurity approach of China, its political, military, and economic incentives, and its attitude towards the U.S. operation in cyberspace (Ismael, 2019)

The Pentagon report reveals that the Chinese military has started dedicating a lot of attention to the cyberspace, especially with the dependence of China on the digital economy increasing. The United States Department of Defense indicates that China is enhancing its cyber capabilities through advanced training and domestic innovation, aiming to close the gap with the United States. The report documents several Chinese cyberattacks and intrusions into American networks, emphasizing that these capabilities are used to support intelligence gathering, economic, military, and strategic, enabling China to build a comprehensive understanding of U.S. defense infrastructure that could be exploited during times of crisis. China's cyber doctrine focuses on future warfare, in which electromagnetic spectrum technologies are employed to disrupt enemy systems, particularly given its awareness of the West's reliance on complex cyber infrastructures. It is widely suspected that many Chinese hackers are either directly affiliated with the military or receive support from Chinese and Russian intelligence agencies.

In recent years, China has unveiled two stealth aircraft reportedly comparable to the American F-22 Raptor and F-35 Lightning II, which are manufactured by Lockheed Martin. (Al-Naba'a News Agency, 2015). This reflects China's technological advancement and rapid progress. U.S. officials believe that cyberspace could become a battlefield between the two countries, especially since their economic interdependence makes conventional warfare less likely.

At the same time, China is investing heavily in cyber defense as a means of reducing the gap with the United States and Russia in traditional military capabilities. Its actions do not confine themselves to dedicated military services like Unit 61398 but rather it seeks to organize civilian cyber militias who are responsible of collecting commercial and industrial secrets to aid the Chinese companies. According to the United States, China is its biggest threat in the sphere of cyber warfare, whereas China also saw the United States as a major cyber threat. Such a perception leads to a higher probability of future cyber conflict and so with the heavy dependency on cyberspace in the operations of state activities and the economy in both nations, there is a possibility of cyber conflict in the future (Noon post magazine, 2025).

The United States accused China of cyber attacks on them, associated with intelligence information theft and espionage missions. Upon discovering that the National Security Agency has been spying on Huawei, the US did not refute these activities. Rather it legitimized them as a component in the attempts to defend U.S. national security. This stand is in the heart of the disagreement between the two nations, meaning that all Chinese companies in the United States are under constant watch by the American security agencies. Both Der Spiegel and The New York Times reported on March 22, 2014, on the same story, using classified files that the National Security Agency had been spying on Huawei over the past seven years, and the amount of data and information gathered by the agency was immense. It also was revealed in the documents that a number of other Chinese institutions were being monitored such as the ministry of commerce, banks, telecommunication companies, and also the former Chinese president Hu Jintao.

Wu Lin, a Director of Public Relations at Huawei responded: What the U.S government has done is precisely what it charges us of. The Der Spiegel also reported that the National Security Agency had managed to infiltrate the company headquarters in Shenzhen since 2009 and gather about 1,400 data records of its customers including sensitive information of its CEO, Ren Zhengfei. It also acquired access to core source codes of some of the company products which are regarded as highly guarded industrial secrets. One of the most successful companies in the global telecommunications technology is Huawei. It was second in the world in providing cyber equipment sales of over $38 billion in 2013. The company delivers services to a larger audience of over a third of the global population not only in tablets and smartphones but also in the telecommunications infrastructure like wireless routers and fiber-optic cables. (www.infizm.com, 2025)

Over the past four decades, China has emerged as a global technological and economic power. It has become the world's second-largest economy and, since 2016, the largest in terms of purchasing power parity. Its GDP has grown 44-fold since 1979, while that of the United States has increased only threefold. Although China is still classified as a middle-income country, it possesses the world's second-largest high-tech sector, as well as the largest internet and manufacturing sectors. It has also made rapid progress in industries such as robotics, artificial intelligence, advanced communications, and electric vehicles. China's development can be divided into four main phases: (Zhang, 2024)

1. From 1978 to 2000: China relied on foreign investment and imports to build its capabilities.
2. From 2001 to 2012: China focused on strengthening domestic innovation, alongside the emergence of major technology companies such as Huawei and Alibaba Group.
3. From 2012 to 2019: China's global rise was driven by initiatives such as Made in China 2025, as well as advancements in 5G networks and artificial intelligence.
4. Since 2020: China has increasingly focused on technological sovereignty, self-sufficiency, and reducing dependence on the United States.

These developments demonstrate that the global system has changed, with new actors emerging alongside the United States.(Abed and Thgeel, 2022). Several major powers now play significant roles in the international system, including Russia, China, Japan, and the European Union, as well as countries such as Brazil and India. These shifts have contributed to increasing competition within a broader global order.(Manati and Alwan, 2024)

Francis Fukuyama explains the importance of building strong states by stating: "*State-building is a critical issue for the international community today.*" Earlier, the International Commission on

Intervention and State Sovereignty (2001) emphasized that *"a cohesive and peaceful international order is most likely achieved through cooperation among active states confident in their global standing."* These transformations have required a redefinition of the nature and essence of American political and security interests in line with rapid global developments.(Alwan et al. 2021)

U.S. decision-makers have grown increasingly concerned that their European allies are no longer capable of competing with or confronting rising powers such as China and Russia. This concern has been reflected in major U.S. security actions, including involvement in the removal of political regimes aligned with these powers, such as the regime of Omar al-Bashir in Sudan and Muammar Gaddafi in Libya, among others. (Alwan, 2022)

China, considered the third most powerful country militarily after the United States and Russia, is working to modernize its armed forces under the leadership of Xi Jinping, with the goal of achieving global military superiority by 2049. This ambition is supported by substantial military spending, which ranks second worldwide. (Al-Anbari, 2022). Consequently, China has advanced under ideological and political frameworks aimed at achieving economic and technological dominance. (Makki, 2025)

At the same time, American concerns have intensified regarding China's growing technological influence, which is viewed as a potential threat to U.S. economic and military superiority. During his first term, Donald Trump, within the framework of his protectionist policies, sought to impose restrictions on companies with more than a 25 per cent Chinese ownership stake when attempting to acquire American technology or invest in sectors related to national security, such as artificial intelligence, microchips, robotics, and encryption. The continued expansion of China's technological capabilities, particularly in artificial intelligence, is expected to further escalate tensions between the two countries, given its wide-ranging applications in both civilian and military domains. (Khalifa, 2025)

The U.S. Department of Defense (Ministry of War) called for increased government spending to counter China's rising ambitions in artificial intelligence. The U.S. government also encouraged improving long-term strategies to consolidate its achievements and enhance its ability to address emerging challenges, while promoting cooperation and understanding with American technology companies. (Al-Ameer, and Al-Kaoud, 2024). The United States has stated that China seeks to acquire sensitive technologies and U.S. intellectual property to strengthen its military capabilities, posing a threat to American security and the economy. (Al-Masawi, 2021). Some Chinese researchers and students, particularly graduate and postdoctoral students at University of Oxford and other universities, may exploit this access to gather information, especially if they are connected to the Chinese military. Consequently, under presidential authority and U.S. immigration laws, entry for these students and researchers has been restricted, with limited exceptions for undergraduates or those not linked to China's civil-military integration strategy, in order to protect U.S. interests and prevent the misuse of scientific research for military purposes. (Proclamation No.10043.)

Given that the general nature of international relations is continuous change due to economic, military, political, and technological developments, shifts in global strategies occur according to changing foreign policy priorities of major powers in response to evolving international conditions. (Al-Kauod, 2021). However, these strategies remain aligned with these priorities, as competition between the United States and other major powers such as China and Russia seeks to fill strategic vacuums. Such competition represents a path to global leadership, granting unique geoeconomic and geostrategic advantages.(Hamoud, 2022). To safeguard its security against potential threats, the United States has engaged in direct competition with China since 2018 through strict industrial policies, including investment restrictions, research and development support, and export controls, particularly in quantum computing, semiconductors, and artificial intelligence. (Kamar, 2025)

The rivalry between the two nations revolves around the following critical matters:

1. Sovereignty and technological decoupling in sensitive industries.
2. Domination of supply chains around the globe, in particular semiconductors.
3. Information security and data control.
4. Setting standards of international standards of high technologies.

Although the economic models are different in both countries, they both promote their top companies and strive to enhance their standards in the international markets. The United States is dependent on the partnership with Europe, Japan, and South Korea, and China is dependent on the Belt and Road Initiative. This competition puts

regional pressures over East Asian nations, especially Taiwan, Japan, and South Korea, who pay attention to balance U.S. assistance and access to the Chinese market, diversify chains of supplies, and enhance domestic capability of innovations. Competition has resulted in an internationally dispersed technology landscape, heightened risks and expenses and is an indication of the coming of a so-called technological cold war that will redefine the global economic landscape in years to come. (Zhang, 2024)

Based on the above, it is obvious that the rivalry between United States and China in cyberspace is no longer only technological or economic but has become a strategic conflict as it has delved into the centre of control in the unipolar international system. The United States has used the idea of national security to block out Chinese companies and even keep them out of high-level technologies, and China has attempted to improve its technological autonomy by creating services in artificial intelligence, semiconductors, and fifth-generation (5G) networks. This competition is an indication of how the concept of power is changing its traditional material aspect to an informational and digital aspect of power, which has transformed the world powers. Competition may lead to a bipolar or multipolar system of technology sooner or later and the leadership of sources of innovation and control of cyberspace would be at the center of the future international balance of power.

Section Two: The Struggle for Dominance over Cybertechnology and Technological Superiority Projects

Although the digital economy is expected to see great industrial advancements owing to the introduction of the fifth-generation (5G) networks, which promise a variety of applications, including autonomous vehicles, smart grids, automated factories, and smart cities, all of which necessitate the use of high-speed communications, this technology is also raising serious concerns to the United States, especially in terms of national security. The reason is that the technical base of the said networks is heavily reliant on Huawei, among the largest 5G network equipment providers in the world, and has strong connections with Chinese government. In this regard, President Donald Trump released the executive order in his first term to prohibit Huawei equipment use in the U.S. networks. This decision was not only aimed at securing the information infrastructure, but it was a part of an overall strategy also covering cybersecurity needs, technical preventive control, and support of research, training, and technological growth (Williams, 2019).

China, in its turn, further enhanced its activities to remain on the same level with this new stage of technological advances, in 5G technologies, which the United States sees as a direct threat to its national security. Huawei is leading in the Chinese industry, ranking second after Samsung in the world in the manufacture of devices and smartphones and which share some 17 percent of the market in 2019. These corporations have experienced a remarkable rise in annual revenues, with a 20% increase in 2018 relative to 2017, reaching approximately $107 billion, compared to a very minimal growth of 12 billion, which makes them compete with large corporations in America like Google and Microsoft (Wan, 2025).

In the early part of 2019, Huawei technologies in the area of 5G set the world performance and evaluation contests and won the award of the best 5G technology in the world summit. This accomplishment heightened the competition between the US and China. The United States in turn declared a boycott of Huawei that would prohibit it from engaging in any contracts or tenders with U.S. territory and pressurize its political and economic partners to keep Huawei out of 5G network development. Other countries, including New Zealand, Australia, and some reluctant ones, including Germany, France, the United Kingdom, and Poland, gave in to this pressure, and others, such as Germany and France, were hesitant because of allegations of the connections of the company founder with the People Liberation Army.

Huawei crisis is an outstanding case of strategic and technological competition between the U.S and China, which is not just on economic level but on a wide geopolitical and security background. (Fakhri, 2019). The blacklist of Chinese companies (primarily Huawei and over fifty others) was introduced during the first term of President Donald Trump, who charged them with stealing intellectual property and spying on the American government on behalf of the Chinese one. (The blacklist is a list of individuals, organizations, or entities that are avoided, excluded, or prohibited as they are deemed unreliable or they engage in unacceptable behavior. When one is on a blacklist in legal and business terms, they have restrictions or penalties imposed on them, such as a prohibition of dealing, a suspension of a licence, or a blockage on access to markets or resources, usually due to security reasons or political reasons or an illegal act. This

gave the U.S. companies no right to do any business with them and deprived them of access to essential technologies like semiconductors and Android operating system (Al-Jazeera, Channel, 2020). Other Chinese companies such as SMIC were not left out of the list as well to restrict the technological advancement of China and promote self-sufficiency in the production of semiconductors. These steps were the basis of the U.S. policy in countering the technological ascendancy of China. (Fakhri, 2019)

The reason why American concerns were related to technology companies in China is due to various factors. The most significant of these is the dominance of Huawei in 5G networks that may be a threat to the national security of the United States, as well as the accusations of espionage and the connections of the founder of the company with the Chinese military. These actions are also a leveraging instrument in the greater trade conflict, to make the most of the U.S. and pressure China in terms of technology and trade dealings. (Williams, 2019)

China on its part sees such U.S. policies as an effort to stall its technological rise and disrupt its Made in China 2025 strategy which puts 5G networks at the core of its future industrial endeavors. The situation intensified when the Chief Financial Officer of Huawei was arrested in 2018, which shows the strategic aspect of the competition that is not just economic anymore. (Al-Lababidi, 2019)

The main U.S. motivations for escalation against Huawei and other Chinese companies can be summarized in four key axes: (Fakhri, 2019)

1. Technological and Economic Rise: Huawei has become the world's second-largest company in tablets and smartphones, achieving revenues exceeding $100 billion in 2018 and profits of approximately $8.8 billion, with sales surpassing 54 million phones. This has made it a major and strategic competitor to leading firms such as Samsung.
2. Espionage and Security Risks: These concerns relate to Huawei's connections with the Chinese government and its efforts to obtain sensitive technologies and U.S. intellectual property.
3. Dominance in the 5G Market: 5G is considered a strategic tool for controlling global digital and critical infrastructure, as well as for collecting vital information about Western countries.
4. Negotiation Pressure in the Trade War: The United States seeks to create obstacles for Chinese companies in order to strengthen its bargaining position and secure political and economic gains in negotiations.

The confrontation also included reciprocal measures, such as restrictions on foreign investments and sanctions on other Chinese companies. Companies such as ZTE were provisional banned to do business with the U.S. markets, which was in a bid to preserve technological advancement and secure American innovation. The Huawei case was a reflection of the geopolitical and technological tension between the two superpowers which reflected the change of competition to a wider platform that includes the dominance of the world in relation to technology, national security, and digital sovereignty (Salah, 2020). (Fakhri, 2019). China is pursuing its technological independence and at the same time attaining its future industrial goals, the United States is dealing with ensuring that there is no dominance of a Chinese takeover of global digital infrastructure and maintaining its leadership role, specifically in 5G networks and the associated technologies, amidst the current diplomatic tensions and tit-for-tats between the two countries. (Abdul-Fattah, 2020). The Huawei crisis depicts that the US China competition has taken the center stage in the geopolitical and technological aspects. Technological restrictions by the United States are applied in protecting the national security whereas China is still seeking the technological independence of itself as part of its industrial policy. This competition indicates how competition in the traditional economy is being moved to the global cyber realm and how the aspects of political and technological power should be balanced so that the competition and stability in bilateral relations can be guaranteed.

CONCLUSIONS

1. The research found out that the U.S.-China competition in the cyberspace has emerged as one of the most notable aspects of geopolitical and technological competition in the 21 st century with both countries competing to strengthen their digital and security topography.
2. Cyber technology has also become a tactic that both states have employed in enhancing their power either by coming up with sophisticated hacking software or locking down their critical infrastructures against possible attacks.
3. The competition does not end in the military sphere, but also covers the economic, commercial, and technological sectors since both China and the U.S. invest in research and development in order to guarantee their digital dominance and safeguard their strategic interests.

4. The results indicate that the two nations use various tools, including hiring of professionals or enterprises and in some cases informal cyber networks, making the rivalry harder and the possibility of hostile takeovers greater.
5. The study indicated that the lack of international regulations on how to control cyberspace heightens risks and the necessity to have laws and regulations to control unethical competition and proper utilization of technology.

CONCLUSION

The rivalry between China and United States in the cyberspace has taken the form of a characteristic of international relations nowadays. This competition is not limited to the traditional economic competition and turns into a strategic competition of technological dominance, digital infrastructure control, and power in the global technological system. This competition has been aggravated by the accelerated growth of advanced technologies especially 5G networks, artificial intelligence, and the semiconductor industries. As the U.S. tries to ensure technological dominance and provide a safe hand in technology security by imposing restrictions and alliances, China is advancing its technological autonomy by producing grand projects and huge investments. Consequently, technological competition between the two powers is likely to reshape global power balances and contribute to the emergence of a new technological order.

REFERENCES

1. Abd Alameer, M. F., & Al-Kaoud, I. S. (2024). The role of regional organizations in building peace in South Sudan: IGAD as a model. *Journal of Ecohumanism*. (Published in Scopus-indexed journals).
2. Abdel-Fattah, F. Z. (2020). *Strategies for confronting adversaries in cyberspace*. *International Politics Journal, 55*(220).
3. Abed, S. S., & Thgeel, A. A. H. (2022). Diagnosing the severity of the Syrian conflict according to Michael S. Lund. *Journal of Positive School Psychology*, 6(5), 6409–6419 (p. 6412). (Scopus-indexed).
4. Al-Anbari, A. A. (2022). *Enhancing competitive opportunities for active powers in the international system: A study on the impact of economic and military variables*. *Tikrit Journal of Political Science, University of Baghdad, College of Political Science*.
5. Al-Bahi, R. (2021, April 18). *Cybersecurity in 2020: Between opportunities, challenges, and protection*. *Algerian Encyclopedia of Political and Strategic Studies*. Retrieved from https://politics-dz.com
6. Albrecht, D. (2021). *Toward cyber realism: No technical solutions to geopolitical problems*. *Independent Arabia*. Retrieved from https://independentarabia.com
7. Al-Dalil, O. (2021). *Digital sovereignty reshaping the world*. *Ahram Online*. Retrieved from https://ahram.org.eg
8. Al-Hurra News. (2025, November 1). *"By hiring criminal hackers"… U.S. officially accuses China of Microsoft breaches*. Retrieved from https://elsiyasa-news.com
9. Al-Jazeera. (2020). *"The bullet has left the gun": Experts say Biden will not retreat from Trump's war on Chinese tech companies*. Retrieved from https://aljazeera.net
10. Al-Ka'ud, I. S., & Al-Khafaji, A. K. (2021). *The application of smart power in the conflict of regional powers in the Middle East after 2011*. *Journal of Political Science, University of Baghdad, 62*. https://jcopolicy.uobaghdad.edu.iq/index.php/jcopolicy/article/view/589/442
11. Al-Khalifa, I. (n.d.). *Dimensions of the Sino-American conflict over technological dominance: The Huawei dilemma*. *Future Center for Advanced Research and Studies*. Retrieved from https://futureuae.com
12. Al-Lababidi, W. (2019). *5G ignites a dominance conflict between China and the United States*. *Al-Zaman Newspaper*, (14123). Retrieved from https://albayan.ae
13. Al-Masawi, W. (2021). *Paths and issues of the U.S.–China conflict*. *Egyptian Institute for Studies*. Retrieved from https://eipss-eg.org
14. Al-Nabaa News Agency. (2015, June 7). *Hacking U.S. computer networks provides a valuable treasure for hackers*. Retrieved from https://annabaa.org
15. Al-Sky News Arabia. (2025). *U.S. plan to respond to Chinese cyberattacks*. Retrieved from https://skynewsarabia.com
16. Alwan, B. H., Qati, S. K., & Ali, I. A. (2021). Iraqi women's leadership and state-building. *Journal of International Women's Studies*, 22(3), 13. (Published in Scopus-indexed journals). Retrieved from https://vc.bridgew.edu/jiws
17. Alwan, S. O. (2022). Economic and security competition between the United States and Russia in

Africa. *Journal of Positive School Psychology*, 6(7), 644–666 (p. 654). (Scopus-indexed).
18. Arrjoun, H. B. (1996). *Outer space and its external uses*. *Alam Al-Ma'rifa Series*. Kuwait: National Council for Culture, Arts and Letters.
19. BBC News Arabic. (2025, November 1). *Why does the West fear China's Huawei telecommunications company?* Retrieved from https://bbc.com/arabic
20. Brands, H. (2020). *On the Russian–Chinese–American cyber conflict*. *Asharq Al-Awsat*, (15366). Retrieved from https://aawsat.com
21. Davis, J. S., II, Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M. S. (n.d.). *Stateless attribution: Toward international accountability in cyberspace*. RAND Corporation.
22. Dollar, D., Huang, Y., & Yao, Y. (2020). *China 2049: The economic challenges of a rising global power*. Brookings Institution Press.
23. Doshi, R., et al. (2021). *China as a "cyber superpower": Divergent views in Beijing on telecommunications* (Executive summary). *Brookings Institution*. Retrieved from https://brookings.edu
24. Fakhri, A. (2019). *The comprehensive deal: Will Beijing negotiate with Washington over the Huawei crisis? Future Center for Advanced Research and Studies*. Retrieved from https://futureuae.com
25. Hamoud, M. F., & Aziz, A. H. (2022). *The impact of the U.S. military variable on the security reality of the Arabian Gulf after 2003*. *Journal of Political Science*, (64), 166–167. https://jcopolicy.uobaghdad.edu.iq/index.php/jcopolicy/article/view/620/499
26. Huntington, S. P. (1996). *The clash of civilizations and the remaking of world order* (T. Al-Shayeb, Trans.; 2nd ed.). New York: Simon & Schuster.
27. Kamar, S. H., & Hamid, H. K. (2025). *The impact of security alliances on conflict dynamics in the Arabian Gulf after 2003*. *Journal of Political Science, University of Baghdad*, (70).
28. Maki, M. J., & Saleh, Y. M. (2025). *The role of identity in competition and conflict between China and India*. *Journal of Political Science, University of Baghdad*, (70), 260. https://jcopolicy.uobaghdad.edu.iq/index.php/jcopolicy/article/view/810/589
29. Manati, T. K., & Alwan, S. O. (2024). Transformations of the world order after the COVID-19 pandemic: The role of culture, science, and the environment. *Journal of International Crisis and Risk Communication Research*, 7(S10), 1815. (Scopus-indexed).
30. New York Times. (n.d.). *China as the primary cyber threat: How it uses sophisticated ghost attacks against the United States*. Retrieved from https://albasalh.com
31. Otkin, A. (2003). *The American strategy for the 21st century* (A. M. Ibrahim, Trans.; 1st ed.). Cairo: National Project for Translation.
32. Salah, A. (2020). *Will the U.S.–China agreement end the trade war? Future Center for Advanced Research and Studies*. Retrieved from https://futureuae.com
33. Schia, N., & Gjesvik, L. (2017). *China's cyber sovereignty (Policy brief)* (p. 1). Norwegian Institute of International Affairs.
34. Segal, A. (2020). *Looking to the future of Sino-Russian cybersecurity cooperation*. Retrieved from https://warontherocks.com
35. Wan, C. Y. (2025). *Why the West fears Huawei*. *BBC News Arabic*.
36. Williams, R. (2019). *The Huawei dilemma: Challenges of securing 5G networks in the United States* .Al-Bahi, R. (Trans.). *Future Center for Advanced Research and Studies*. Retrieved from https://futureuae.com/ar/Mainpage/Item/4955
37. Zhang, K. H. (2024). Geoeconomics of US–China tech rivalry and industrial policy. *Asia and the Global Economy*, 4(2). Retrieved from https://www.sciencedirect.com/science/article/pii/S2667111524000227