SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 49-57
Open Access. Online & Print

DOI: 10.5281/zenodo. 12426105

KEY DETERMINANTS OF CYBERSPACE UTILIZATION IN U.S.–CHINA RELATIONS AFTER 2012

Huda Khalaf Ali Ahmed[1]*, Halah Khalid Hameed[2]

University of Baghdad/ College of Political Science

Received: 01/12/2025
Accepted: 02/01/2026

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

ABSTRACT

After 2012, the cyberspace has become the most important arenas of strategic competition between the United States and the People Republic of China. This rivalry involves three pillars that are central to it including artificial intelligence (AI); data, information, and digital infrastructure; and cybersecurity. The creation of advanced algorithms, autonomous systems, and improved offensive and defensive cyber capabilities has become the main basis of technological and military dominance and is driven by AI. At the same time, digital information and data are a crucial resource to which both states base their power-building strategies. The United States is also dependent on major technological companies across the world and has the largest data reserves in the world, but China is building massive digital infrastructures (including 5G wireless networks) and building the strength of its computing hubs and supply chains. Parallel to it, cybersecurity has turned out to become the principal front on which the two powers confront each other. The United States advocates an open internet model, whereas China is guided by the concept of the so-called cyber sovereignty, not to mention the creation of superior offensive and defensive doctrines. As such, cyberspace has ceased being an area of operation to being a determinant of international power, contributor to economic development as well as national security of the two nations.

KEYWORDS: The United States, China, artificial intelligence, digital infrastructure and information, cybersecurity.

1. INTRODUCTION

The fact that cyberspace has become an important sphere where states attempt to advance their force in the traditional spheres that form the pillars of the statehood, including political, military, economic, and demographic, is evident. Most states are becoming more and more competitive and trying to dominate and manage this sphere and as a result of their greater geopolitical disputes. This rivalry is especially noticeable in the case of the United States and the People's Republic of China, which are eager to exercise their control over the sphere of cyberspace in terms of their bilateral strategic competition.

Surprisingly, it is China that has seen impressive progress in the military, technology, and economy, particularly, in cyberspace, artificial intelligence, data systems, and computer infrastructure. The developments have made China a powerful force in this strategic field.

2. RESEARCH PROBLEM

1) What are the basic elements behind the use of cyberspace in U.S China relations since 2012? But what has artificial intelligence, cybersecurity, data, and the digital infrastructure done to this type of rivalry?
2) This key question separates into a set of questions:
3) What has the United States and China done to leverage artificial intelligence to augment their cyber power?
4) What has cybersecurity done to calm down or intensify the competition between the two powers?
5) What is the role of digital infrastructure and data in forming their strategic interactions?

3. HYPOTHESIS

China and the United States use cyberspace in the post-2012 period with three major blocks as its foundation, including artificial intelligence, data and digital infrastructure, and cybersecurity. These elements have also added to the political, security and economic rivalry between the two powers.

4. ARTIFICIAL INTELLIGENCE

To prove that the world order has changed, there are new actors on the international stage alongside the United States of America ([Abed&Thgeel, 2022]).As evidenced by showing that the global system has evolved, and that new actors have risen beside the United States, major powers have acquired large portions of global resources of power now. These are Russia, China, Japan, European Union and the emerging powers like Brazil and India. Collectively, they constitute substantial pillars of the international power structure.

Shifts in the global order have thus contributed to the emergence of broader and more intense competition among states.The transformations in the global system have led to increased competition among states within a broader global framework (Tamara Kadim Manati, Saad Obaid Alwan, Transformations of the World Order after the Corona Pandemic COVID-19: The Role of Culture, Science, and the Environment, Journal of International Crisis and Risk Communication Research, 2024, Vol. 7, No. S10, p. 1815, research published in the Scopus database. For more information, see:

https://jicrcr.com/index.php/jicrcr/article/view/1154/924) Francis Fukuyama explains the true importance of building strong states, stating, "State-building is a critical issue for the international community today." The International Commission on Intervention and State Sovereignty (ICISS) report (2001) had previously affirmed that "a cohesive and peaceful international order is most likely to be achieved through the cooperation of effective states, confident in their place in the world." [Batool Hussain Alwan1, Sana Kadhim Qati2, Inass Abdulsada Ali, Iraqi Women's Leadership and State-Building, Journal of International Women's Studies, Volume 22, Issue 3, Women's Studies: The Possibility of Rethinking and Designing the Foundations of Modern Culture, April 2021, p. 13.] This research is published in the Scopus database. The international system is based on a pattern of alliances between major powers and is influenced by the balances of power in international relations.The temporary nature of the international system often leads to the emergence of a new system due to changes in the global landscape. [Tamara Kadim Manati1, Dr. Saad Obaid Alwan2, Transformations of the World Order after the Corona Pandemic COVID-19: The Role of Culture, Science, and the Environment, Journal of International Crisis and Risk Communication Research, 2024, Vol. 7, No. S10, p. 1811. Published in Scopus.

Artificial intelligence is the most powerful and significant technologies available to humanity in the modern era. Neglecting it constitutes a grave strategic error. Leaders of states and major corporations agree that AI presents enormous opportunities for improving various aspects of life, while posing serious challenges for those who fall behind. For this reason, many states have adopted clear national strategies for the development of this advanced technology.

This interest in the United States started in 2016 under the rule of the former President Barack Obama with the first comprehensive report on artificial intelligence named Preparing for the Future of

Artificial Intelligence. The backing of AI remained during the administration of President Donald Trump who initiated the program Artificial Intelligence for the American People, with the focus on the fact that the world is entering the new technological revolution that would change the lives and create vast wealth.

Kai-Fu Lee argues that China, along with its largest investors, have invested enormous amounts of money in creating AI technologies. It has greatly increased the quantity of students who are being sent overseas to undertake innovation and artificial intelligence. According to Lee, China had taken almost 48 percent of AI investments worldwide by 2017 and became a leader over the United States. China made it its goal to become the primary hub of AI innovations in the world by 2030.Although United States, Canada, and the United Kingdom previously took the lead in AI research, the change in the balance occurred as China initiated intensive investments starting in 2016. According to the explanation provided by Kai-Fu Lee, the evolution of AI follows a series of steps: after the discovery stage, there is the application stage that involves the involvement of experts to guide and use findings, and the data stage. Instead of discovery, the application stage was the priority of China, taking advantage of the favor of the Chinese companies and labs, even those ones that work in Silicon Valley. This policy greatly increased the competitiveness of China in the sector.

The US aims to maintain its world dominance speeding up the development of research, widening the area of artificial intelligence usage, and training human resources that are ready to utilize this technology. China, on the contrary, has been pursuing one of the most ambitious and all-inclusive approaches in the world, aiming to become the most powerful in AI in the world by 2030 with enormous investment and a strong digital network. World technology leaders emphasize the disruptive importance of AI. According to Jeff Bezos, Amazon founder, the current age is the golden age of artificial intelligence, which is able to solve the problems that were deemed as science fiction a few years ago. Co-founder of Google Sergey Brin considers AI to be the most significant advancement in computing in his lifetime. The same ideas are expressed by Microsoft CEO Satya Nadella who says that AI is going to fundamentally transform the future of work and society. Both Klaus Schwab, the founder and executive chairman of the World Economic Forum, and many scholars and experts, are of the opinion that artificial intelligence, and in particular, when combined with other technological advances, has sparked the Fourth Industrial Revolution, which is likely to cause far-reaching changes not only in the economic but also in the social sphere.

Johnson makes a comparison between the strategic orientations of the two countries namely Russia and China towards the complete integration of artificial intelligence into their military systems. As he argues, it is extensively established that both states have integrated AI technologies in their nuclear and ballistic missile arsenals such that the weapons will react instantly in case of a threat. Such systems might automatically carry out retaliatory attacks which were pre-programmed once an incoming attack is detected.

On the other hand, according to Johnson, the United States has assumed a more reserved and ethically based policy in that it would rather leave the decision-making process in the hands of human beings as a part of its defense architecture. He cautions though that such a technique may lead to complicated results in the future crises. According to Johnson, the high pace of AI technologies development will have a significant security issue, and the most significant one will be the loss of international order and the new arms race with its focus on highly sophisticated AI-driven weapon systems. Despite the continued superiority of states in the traditional balance of power, the gap between them and non-state actors is shrinking ([- Sabah Abdel Sabour Abdel Hai, The Use of Electronic Power in International Interactions: Al-Qaeda as a Model, Part One, Egyptian Institute for Political and Strategic Studies, Political Studies, 2016, pp. 3-4.]).

Christian Brose argues that the United States, over the past two decades, has been preoccupied with its wars in the Middle East, while its competitors—primarily Russia and China—were studying U.S. military strategy and identifying its vulnerabilities to develop effective means of surpassing it. China has already embarked on major national projects designed to place it at the forefront of technologically advanced nations, especially in AI.

Brose notes that these trends reflect a rapid erosion of U.S. military superiority. A 2017 RAND Corporation report warned that the U.S. military could lose the next major conflict it is forced to fight. Similarly, a warning was given in the same year by the Chairman of the Joint Chiefs of Staff, General Joseph Dunford who said:

We are losing our qualitative and numerical advantage in case we do not shift our course in the coming few years.

Brose continues with the fact that more troubling is the fact that the conventional deterrence power of

United States is eroded. In case Chinese or Russian leaders develop the idea that they may win in the military conflict against the United States, they may resort to more aggressive and dangerous strategies. This may take the form of political or military investigations of American allies -to shake their faith in American security- in such spots as the Baltic states, South Korea, Taiwan, the Philippines or Japan.

In this case, China and Russia would be able to increase their power in the world without having to face each other, relying on the strategic principle of Sun Tzu:

To overcome the enemy without engaging in battle is the art of skill.

5. INFORMATION, DATA AND DIGITAL INFRASTRUCTURE

Cyber infrastructure is a very essential aspect of daily lives of individuals and organizations in the era of the digital age. It is now impossible to conceive of the operation of the contemporary institutions and businesses without the utilization of highly sophisticated and hi-tech systems of computation, cloud storage, and interconnected networks. Cyber infrastructure has become the backbone in most of the activities that are very important such as information management, data exchange and implementation of governmental and business activities.

Such online applications have rendered cyber infrastructure to be a core need when it comes to business continuity in different sectors. With the growing dependence on digital systems, it is no longer enough that the systems are only efficient or that they have the capability of processing the data and providing services at a high level. It has also become imperative to protect them against the external threats. Nonetheless, even with all the significant advantages, cyber infrastructure still has very low security levels, be it targeting specific computer attacks or technical outages leading to the loss of data or system-related overloads.

These threats are very challenging not only on the technical level but also on the security, economic, and social levels. Cyberattacks can disrupt markets, hamper the provision of vital services, including air transport, money transfers, commerce, and even the social fabric ([- Asif Al-Khalidi, The Coming Cyber Wars: Goodbye to Conventional Weapons, Excavations, research published on the World Wide Web (Internet), for more information see: The Coming Cyber Wars: Goodbye to Conventional Weapons), as well as healthcare, transportation, and energy, and disrupt the confidence of the population. This has resulted in the cyber infrastructure being a pressing need and top agenda on national and international security issues.

The cyber infrastructure is as robust as the elements that make it up, and any attacks might cause disruption of important systems like the power grid or the telecommunication system. These destabilizations are a major challenge to the national interests, economic stability, and the safety of the people. Protection of this infrastructure is thus crucial in ensuring privacy, development of trust among the population and ensuring that essential services are not disrupted. With the threats continuously posed by the hostile states, organized groups, and individual hackers, the measures of cybersecurity need to be enhanced, more adaptable and constantly revised to pace up with the changing adversaries.

The U.S. government has started paying serious attention to cyber threats starting in the year 1998. Under the leadership of President Bill Clinton, the U.S government realized the danger of cyberattcks and established it as a national security threat that was increasing. In the period between 1998 and 2001, the United States developed strategic reports in relation to the national security, with special emphasis on critical infrastructure protection against the emergent digital threats.

In this frame, the U.S. Department of Defense created the Joint Task Force-Computer Network Defense (JTF-CND) as the structure that entails the counteraction of cyberattacks and defensive and offensive actions in cyberspace. Things however changed and the duties were divided with the defense information systems agency (DISA) handling defensive cyber missions and the national security agency (NSA) taking charge of offensive cyber capabilities.

In 2009, as a larger reorganization of U.S. cyber capabilities, these were all brought together in a single unified entity: The United States Cyber Command (USCYBERCOM), which was to replace any central location of military operations in cyberspace.

The U.S. government led by President George W. Bush came to realize the severity of the emergent, non-traditional threats to the American national security after the events on September 11, 2001, in the form of information warfare and cyberattacks. It became quite clear that such threats had to be dealt with in a decisive way and through proper strategies especially because the adversaries and potential competitors were starting to build up the capability to use cyber tools as a means of countering the U.S. influence.

The initial official warning on these dangers was published in the Department of Defense report presented to the Congress in 2001, which contained the observations made by the then-Deputy Secretary of Defense Paul Wolfowitz. He stressed on a dire necessity of the United States to assume a novel defensive tactic

that can deal with non-conventional kinds of warfare in particular those that belong to what he described as the Global Information Network Warfare.

In 2003, the presidential directive was expressed since it is evident that there is a great need to tighten the security of information within the computer networks that are interrelated with the national infrastructure as the networks are characterized as the weakest link in the national security framework and most susceptible to any cyberattack. Still on this path, in November 2007 the Bush administration asked the National Security Agency (NSA) to liaise with the Department of Homeland Security (DHS) to ensure that the governmental and civilian networks are safeguarded against cyber intrusions- a move that was integrated into a greater national strategy of improving cybersecurity and counterterrorism resources. This initiative was financed by the federal government using federal funds to the tune of $144 million under a greater initiative to strengthen the information infrastructure of the institutions of the U.S. government.

As the issue of cyber-attacks on U.S. troops intensified in 2008, President Barack Obama made cyber threats one of the gravest dangers to the United States and termed the means of the cyber war as the real weapons of mass destruction. Here, the Department of Defense made it known that any massive cyberattack that leads to a significant harm to the United States may be treated as an act of war which means that the United States may respond by conventional warfare- not necessarily by a counter-cyberwar.

As a result, the government of the U.S. initiated the project of Comprehensive National Cybersecurity Initiative (CNCI), which became a strategic milestone in the development of cyber defense in the USA. The campaign was allocated about $8 billion in the federal 2009 budget and intended on coming up with national cybersecurity capabilities as well as improving the preparedness of the governmental institutions to face the ever-increasing digital threat environment.

In the same year, the United States declared the formation of a special command which focuses on the activities in cyberspace so that the U.S. Armed Forces and its virtual networks could be secured, and critical national infrastructures could be defended against more sophisticated cyberattacks. President Barack Obama put a great emphasis to the issue of cybersecurity, as he regarded it as one of the most acute issues to the national and economical security of the U.S.

To this end, President Obama commissioned a specialized team to conduct a comprehensive review of previous cybersecurity policies and strategies. This effort culminated in the preparation of a report titled "Cyberspace Policy Review", which—based on extensive assessments and consultations—recommended a set of urgent measures to strengthen U.S. cyber readiness and strategic posture.This makes it one of the most dangerous forms of warfare in the modern era ([- Asif Al-Khalidi, The Coming Cyber Wars: Goodbye to Conventional Weapons, Excavations, research published on the World Wide Web (Internet), for more information see: The Coming Cyber Wars: Goodbye to Conventional Weapons | Excavations, last visit on Saturday, September 13, 2025.]). The United States adopts a deterrence policy based on the principle of responding in kind (by any means appropriate to the extent of the damage), a principle grounded in international law and the right of states to defend themselves against cyberattacks ([Joseph S. Nye Jr., "Is Cyber Weapon the Ultimate Weapon?", an article published on Al Jazeera, July 10, 2018, available online at: Is Cyber Weapon the Ultimate Weapon? | Viewpoints | Al Jazeera Net (aljazeera.net), last accessed April 28, 2025, available as a PDF file]). The threat of deterrence may be one of the reasons that has thus far prevented a major cyberattack leading to a collapse of infrastructure or a complete power outage ([Ibid.]).

The team finally came up with a report which was christened The Cyberspace Policy Review which contained the analysis and suggestions meant to enhance the national response to the digital threats. Based on this strategic path, the U.S. had created a new military command, the U.S. Cyber Command (Cybercom) to coordinate the efforts of defending the country by building infrastructural resilience and improving the capability of the country to deter and counter cyberattacks. As of 2014, the Command has been allocated more than a lot of money than it had been in the past years due to the increased strategic value of cybersecurity as part of the U.S. defense policy.

According to a report prepared by the Pentagon evaluating the capability of the Chinese military, it was observed that over the past few years, China has increasingly concentrated on cyberspace, owing to the fact that it has been increasingly depending on the digital economy. The 2017 Annual Report also made direct allusions to the China cybersecurity strategy, in which Beijing stated that it was increasing the pace of modernizing its military cyber capabilities as one of the key pillars of national defense. The report also brought out that China has realized that it has weaknesses in its cyber capabilities in relation to that of the United States and has made an attempt to close this divide through training, nurturing internal innovation and specialized cyber capabilities.

It was also indicated in the report that China has greatly increased its operations on offensive cyber

operations, including its targeting of the U.S. government computer systems. Pentagon claims that the main aim of these operations is to penetrate the cyber networks to gather intelligence, economic information, military, diplomatic, and even academic information. The report indicated that such data has been utilized to create an overall picture in the cyber warfare units of the People's Liberation Army of the U.S. defence systems, military capabilities and supply chains, a strength that China can use in case a crisis arises.

It was reported that the United States still has a long way to go in creating the right model to ensure cyber deterrence, especially when it comes to combating the growing operations of China and Russia in the same field.

Such dynamics required the redefining of the political and security interests of the United States in such a way that was in line with the fast changing developments in the world. The American policy makers were becoming more and more concerned with the fact that their European allies could no longer compete or counterbalance with the emerging international powers, the most powerful of whom were China and Russia. This fear became materialized in landmark American security-related initiatives that saw the ousting of political regimes that had allied themselves with Beijing and Moscow like the Omar al-Bashir government of Sudan, the Muammar Gaddafi government of Libya and others.

It means that there is an increased focus on the modernization of the future plans of warfare in the Chinese cyber-military doctrine, especially on the premise of being able to control the electromagnetic spectrum. China, it seems, is gearing up to fight in the future by using sophisticated cyber equipment, methodically shutting down the access of its enemies to the key areas of cyberspace, particularly the United States. China is more than aware of how much the western states, led by the United States, depend on information-technology infrastructure as a result, Beijing is targeting the centers of gravity in the systems, which gives China a unique strategic edge.

Similarly, in the recent past years, China has also demonstrated two stealth-tech fighter planes, which experts believe are similar in terms of power to the American F-35 and F- 22 produced by Lockheed Martin. Such a development highlights the attempts of China to reduce the technological gap with the United States in the aerial sphere as well. Different news companies have quoted a Chinese strategist saying: "With the help of computers, our armed forces can now afford long-range surveillance, and the more accurate, powerful, extended-range attacks.

The United States, in its turn, did not stand on the back seat. President Obama, in his former presidential role, issued Presidential Directive No. 20, which ordered the U.S intelligence agencies to develop a list of cyber sites that would need special protection within the U.S territory in the event of a cyber-attack. Critical infrastructure in cyberspace is the physical structures and cyber systems that are critical to the operations of the society, the economy, and the national security of the state. The Australian Cyber Security Centre says that any denial or harm to this infrastructure seriously harms the welfare, security, and defense capabilities of a state-making the conventional security approaches insufficient, and innovating cyber-defense methods is the only way to go.

Essential infrastructure constitutes the foundation of the social operations and the overall welfare of the society in any country. As technology and information systems expanded, it has expanded its activities to cover the public utilities besides the national-security fields. The global information infrastructure is not the same as cyber infrastructure because it includes the data-processing and data-transmission infrastructures which include the satellite, the internet and wireless. The security of cyber-infrastructure can therefore be said to be the security of data and devices against breach and attacks. As reliance on the Internet of Things, cloud computing, and the digital is growing, these systems are continuously under threat, which may lead to both economical and human damage. Hence, their safety and sustainability are the key to the continuity of critical services.

As the world has become increasingly reliant on information and communications technology, the possibility of cyberattacks against critical infrastructures has also grown considerably. Although it is not known clearly what cyber warfare is, the incidents on countries like Georgia, Estonia, Iran, the United States and South Korea depict the magnitude of this menace. There were also instances of cyber intrusions that are related to widespread power outages in Brazil that caused traffic-control systems, metro operations, and the Itaipu Dam to come to a halt, affecting over 60 million people. Airport systems too have become targets and this has resulted in the interference of the critical systems including that of lighting and communications. Cyberattacks have been reported to occur in over 30 private-companies and six states in less than a period of time, which emphasizes the intensity of such threats. However, such risks are manageable with the increased level of cybersecurity, the creation of safe practices and standards, and the improvement of international cooperation to protect civilians and preserve the survival of digital services and infrastructure.

Another area of cyber warfare is the targeting of critical infrastructure and military systems such as SCADA networks, smart grids, by allowing hostile states to launch attacks on par with those of traditional warfare through cyber weaponry, such as viruses, worms, logic bombs, jamming devices, cyber data-collection operations, wireless data transmissions, electromagnetic-pulse weapons, malicious or counterfeit software, embedded Trojan timing networks and computer reconnaissance systems. Despite the fact that smart grids are more energy efficient, they become good targets of cyberattacks due to their connection to the internet.

The devices used by attackers to spread malware that could harm or cripple energy networks include smart meters. Although these systems have been tried to be digitalized, attacks are daily in many countries and can lead to long disruption of operations since it is hard to replace essential equipment and hence losses of money are incurred in a lot of ways. Cyber warfare can therefore be used as a tool to temporarily shut down operations of a state or coalition without having to engage in a conventional military clash, in an attempt to achieve certain strategic goals. Taken together, these problems result in situations where interstate conflicts may arise or intensify.

6. CYBERSECURITY

The cost and immense losses that characterize these attacks has made the need to protect systems against internal and external attacks a priority to institutions, individuals, and states. The majority of cyberattacks are commitments by the state sponsored actors, terrorist organizations, or criminal gangs, and are often associated with theft or leakage of confidential data. Cybersecurity has a different meaning in different states: the United States has Cyber Security and is associated with networks and digital technologies, Russia and China use a more inclusive concept of Information Security which covers both technologies, data, and its use.

Information security describes a set of policies, procedures and controls that are developed to protect data by ensuring four vital principles that include confidentiality, integrity, availability and authentication. This is captured in a number of layers, such as the physical security, data security, operational security, and content security. Nevertheless, this customary definition of information security is only partial because it is more technical and does not capture the multidimensional aspect of cyberspace- so it is important that this concept is extended to capture the wider areas of cyber space and threats.

Cyber domain security is the protection of communication networks, electromagnetic systems and devices, and operational data applications against the threat of both internal and external attackers.

It is not confined to the protection of internet communications, instead, it is stretched to the protection of economic, political, cultural, social, and defense-related security of a state. Cybersecurity can also be understood as safeguarding digital resources both hardware and software against unauthorized access to maintain the confidentiality, integrity and availability of information. In addition, cybersecurity can be defined as the process of ensuring the communication channels and digital devices are not attacked by external or internal parties giving high standards of protection that denies hackers access to the devices hence protecting the institutions and individuals against monetary, technical, and political attacks.

The cybersecurity has become a significant part of the policies of the national security, with the major powers, such as the United States, the European Union, China, Russia, and India, considering it one of the top priorities in their defense policies. The changing nature of national security due to the increasing threats posed by the cyberspace has seen the definition of the concept of national security extending its scope to involve the protection of the cyber space against intrusion and malicious cyber activities.

7. CONCLUSION

This paper has proven that cyberspace has turned out to be a determinant in the relationship between the U.S. and China beyond 2012. The strategicization of cyberspace is based on three main pillars:

Artificial intelligence has become one of the strategic tools of increasing the economic and military capabilities; digital infrastructure and data have become central components in the struggles to gain influence in the global digital economy; and cybersecurity has become a highly sensitive axis that reflects the growing tensions between the two states as the number of cyberattacks increase and the policy of fortification and deterrence grows.

The results also suggest that the dynamic between these factors has escalated the strategic competition between the United States and China, so that the cyberspace has become a region of geopolitical rivalry whose consequences go beyond the national economy, global politics, and national security structures. Furthermore, the paper makes a conclusion that the further technological progress will only aggravate this competition in the future and redefine the dynamics of power between the two states.

REFERENCES

Abdel-Hay, S. A. A. (2016). The use of cyber power in international interactions: Al-Qaeda as a case study (Part 1). Egyptian Institute for Political and Strategic Studies.

Abdul Latif, S. M. (2015). War in the digital space: A future vision. Risalat Al-Huquq Journal, 7(2).

Ahlqvist, M., & Van, V. (2023). Cyber physical security and critical infrastructure: Protecting nations and societies in the era of connected systems and hybrid threats. CoESS & International Security League.

Ahmed, H. K. A., & Jalal, M. M. (2020). The future of Iraqi–Turkish relations in light of the water variable. Multicultural Education, 7(10).

Al-Ali, A. Z. (n.d.). Previously cited source.

Al-Bahi, G. (2018). Cyber deterrence: Concept, challenges, and requirements. Journal of Media Studies, 1. Arab Democratic Center.

Al-Khalidi, A. (2025, September 13). The coming cyber wars: Farewell to traditional weapons. Hafriyat.

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), 1–13.

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.

Andress, J., Winterfeld, S., & Ablon, L. (2019). Cyber warfare: Techniques, tactics and tools for security practitioners. Syngress.

Annabaa News Agency. (2015, June 7). Hacking American computer networks provides a valuable treasure for hackers. Retrieved March 23, 2025, from https://annabaa.org

Brooks, C. (2019, May 19). Future wars: How Washington maintains its military superiority in the age of artificial intelligence (M. M. Al-Sayyid, Trans.). Future Center for Advanced Research and Studies.

Buskirk, E. V. (2007, August 7). Denial-of-service attack knocks Twitter offline. Wired. https://www.wired.com

Colarik, A. M. (2006). Cyber terrorism: Political and economic implications. Idea Group Publishing.

Dar Al-Jalil for Publishing and Distribution. (2013). Automated control warfare: The fifth weapon of war (1st ed.). Dar Al-Yazouri Scientific Publishing.

Davis, J. (2007, August 21). Hackers take down the most wired country in Europe. Wired.

Fahrenbacher, K. (2009, October 9). 10 things to know about smart grid security. Earth2Tech (Gigaom). https://gigaom.com

Fang, B. (2018). Cyberspace sovereignty: Reflections on building a community of common future in cyberspace. Springer Nature.

Ghaidan, S. G., & Jalal, M. M. (2021). Cyber warfare technology and international confrontation strategy (1st ed.). Adnan Library for Printing and Publishing.

Helft, M., & Jacob, A. (2010, January 13). Google, citing attack, threatens to exit China. The New York Times. https://www.nytimes.com

Inductive Automation. (n.d.). What is SCADA? Supervisory control and data acquisition. https://inductiveautomation.com

Jason, J. (2019). The impact of artificial intelligence on the global arms race (S. A. Salem, Trans.). Future Center for Advanced Research and Studies.

Johnson, T. A. (n.d.). Cybersecurity and cyber warfare. CRC Press.

Lee, K.-F. (2019). The imitation approach: Lessons from Chinese superiority in artificial intelligence (Y. Ayman, Trans.). Future Center for Advanced Research and Studies.

Maileria, M. (2009, November 15). Brazil's next battlefield: Cyberspace. Foreign Policy Journal.

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), 1811–1819.

Marr, B., & Ward, M. (n.d.). Artificial intelligence applications: How fifty successful companies used AI and machine learning to solve problems (A. Yakan Haddad, Trans.). Al-Obeikan Publishing House.

Meeuwisse, R. (2015). Cybersecurity for beginners. Ictutrain Ltd.

Mustafa, Y. M. Y. (n.d.). The United States strategy for cybersecurity. College of Political Science, University of Mosul.

Nye, J. S., Jr. (2018, July 10). Is cyber weaponry the optimal weapon? Al Jazeera.

Pennell, J. (2010, February 5). Securing the smart grid: The road ahead. Network Security Edge.

http://www.networksecurityedge.com
Ranger, S. (2018, August 17). China aims to narrow cyber warfare gap with US. ZDNet.
Ryder, R. D., & Madhavan, A. (2019). Cyber crisis management: Overcoming the challenges in cyberspace. Bloomsbury.
Sarker, I. H. (2024). AI-driven cybersecurity and threat intelligence. Springer Nature.
SentinelOne. (n.d.). Cybersecurity 101: What is cyber infrastructure? SentinelOne.
Sofaer, A. D., & Goodman, S. Y. (2001). The transnational dimension of cybercrime and terrorism. Hoover Institution.
United States Department of Energy. (n.d.). Smart grid. https://www.energy.gov
White, C., & Mazanek, B. (2019). Understanding cyber warfare: Politics, policy and strategy. Routledge.
Abed, S. S., & Thgeel, A. A. H. (2022). Diagnosin The Severity of The Syrian Conflict According to Michael S. Lund. Journal of Positive School Psychology(5), 6409-6419.