



Social Sciences Spectrum

A Double-Blind, Peer-Reviewed, HEC recognized [Y-category](#) Research Journal

E-ISSN: [3006-0427](#) P-ISSN: [3006-0419](#)

Volume 03, Issue 04, 2024

Web link: <https://sss.org.pk/index.php/sss>



Check for updates

Sino-US rivalry: Expansion of Cyberspace Influence on Iran

Rameen Akram

M.Phil Scholar, Department of Political Science and
International Relations, University of Management
and Technology, Lahore, Punjab, Pakistan

Correspondence: rameenak114@gmail.com

Article Information [YY-MM-DD]

Received 2024-11-23

Accepted 2024-12-26

Citation (APA):

Akram, A. (2024). Sino-US rivalry: Expansion of Cyberspace Influence on Iran. *Social Sciences Spectrum*, 3(4), 443-458. <https://doi.org/10.71085/sss.03.04.193>

Abstract

This paper describes how the emerging Sino-U.S. rivalry shapes Iran's cyber capabilities, as well as its broader ramifications for the region. It evaluates Iran's emerging partnership with China, which serves to bolster Tehran's cyber defense and economy but raises its tensions with rival regional powers in Israel and Saudi Arabia. Through this research, there is an effort to understand this regional cyber arms race that originates from U.S. sanctions imposed on Iran as well as assistance from China. The study concludes that the Sino-U.S. Rivalry will continue to play a role in shaping Iran's cyber policies and regional dynamics in the context of a fragmented global cyberspace and increased geopolitical competition. The research makes use of neorealism, the security dilemma, and constructivism as theoretical models to contextualize Iran's strategic decisions in the larger contest between Sino-U.S. global supremacy. China's initiatives, such as the Digital Silk Road, have enabled Iran to acquire crucial telecommunications infrastructure, cybersecurity tools, and high-tech technologies that it requires to survive U.S. sanctions and cyber-attacks. The studies suggest that the collaboration brings short-term technological and economic advantages, increases the dependence of Iran on Beijing, limits Iranian flexibility around the world, and increases regional and international tensions.

Keywords: Sino-US rivalry, Cyberspace influence, Artificial intelligence (AI), Security dilemma, Cyber-attacks.



Content from this work may be used under the terms of the [Creative Commons Attribution-Share-Alike 4.0 International License](#) that allows others to share the work with an acknowledgment of the work's authorship and initial publication in this journal.

Introduction

The title "Sino-US Rivalry: Expansion of Cyber-Space Influence on Iran" encapsulates the central themes of the document, highlighting the interplay between the geopolitical competition between China and the United States and its implications for Iran. The tension of shifting global dynamics from unipolar to multipolar has intensified in recent years which has made both nations seek to expand their global influence and assert dominance in key regions, including the Middle East. The title highlights the ongoing competition and tension between China and the US, which has led to the expansion of their information technology and cyber world influence in various regions, particularly in Iran. When it comes to the Middle Eastern region despite volatile politics, lack of cooperation among states, war-torn shattered economies, this region holds the utmost importance to both US and China, both states encourage the importance of trade and economic cooperation with these middle eastern states as it consists of enormous oil and gas resources, influencing the world economy. The Gulf states are increasingly adopting advanced technologies to diversify their economies, enhance their digital capabilities, and improve their overall competitiveness on the global stage.

The United States has portrayed a policy of offensive realism towards China since the beginning. If we talk about its policies regarding the Sino-US rivalry and implications for Iran, it can include both defensive and offensive realism because of its preemptive and expansionist nature along with diplomatic and cooperation for Iran. They have initiated digital diplomacy through soft power activities and engage people using technology. Here, they also curb anti-Americanism extremism and work for favorable public opinion regarding America. The United States recognizes the pace with which the Internet space has transformed its new security risks. The nation has revised foreign policies for a changed age by protecting itself through appropriate strategy that brings the U.S. strategy to apply both technology and diplomacy with appropriate equilibrium and impact. It further highlights that there is a need to emphasize focusing on cybersecurity within its policy framework (Baycar, 2023). Despite all its policies, U.S. has never been considered a just and fair mediator in Middle Eastern conflicts, given its close relations with Israel and its animosity towards Iran. The United States has adopted a multifaceted approach to counter China's growing influence, which has significant implications for its policy towards Iran.

U.S. Policy Towards China:

The United States has developed a multi-layered approach against China's expanding influence by looking at the economy, technology, military, and diplomacy. The U.S. has imposed tariffs and sanctions on imports from China in order to rectify trade imbalances and protect American industries. These sanctions start under the presidency of Donald Trump and were pursued by Biden targeting the major industry sectors, from electronics to agricultural sectors and restraining China from more advanced technologies, like access to semiconductors, for example. More in technological words, innovation in technology, protection of cyber assets, have given priority, spending billions on investment in R and D in protecting its supremacy than China. For example, programs like the CHIPS (a revitalization effort of the U.S semiconductor industry) and Science Act have improved domestic semiconductor manufacturing capacity. Partnerships with allies have checked China's increasing global technology initiatives-the Digital Silk Road. Militarily, the United States has increased its footprint in the Asia-Pacific region to push back against China's military assertiveness and expansion of dominance, especially in contested areas, such as the South China Sea and Taiwan. This includes deploying further forces and improving alliances to protect

regional security. Diplomatically, the United States has acquired many allies as well as allied and partnered those allies in setting up a united position against China.

Implications for Iran:

The United States has embraced a general approach to counter Iran's activities, focusing on sanctions, regional stability, and energy security. Sanctions are an important tool in US policy, aimed at controlling Iran's nuclear program and restricting its regional impact. These restrictions target important industries such as Iranian banking, oil exports, and military development, putting economic pressure on Tehran to dissuade acts that threaten U.S. interests. Furthermore, the U.S. is also concerned with Iran's backing of proxy forces in the Middle East, such as Hezbollah in Lebanon and other militias in Iraq and Syria, which contribute to regional instability and undermine the security of U.S. allies. The U.S. has therefore strengthened partnerships with regional powers, such as Israel and Saudi Arabia, to contain Iran's influence. In addition, energy security remains an important concern for the U.S. that aims to reduce global dependence on Iranian oil and gas by promoting alternative suppliers and energy diversification. These steps aim, therefore, not just to reduce Iran's economic influence but also to stabilize global energy markets. All these different strategies show, therefore, a continuing U.S. effort to push back against Iran's influence while pushing forward on broader strategic goals in the Middle East and elsewhere.

The U.S. strategy towards China has an indirect impact on its policies toward Iran because both countries are seen as part of a massive geopolitical competition. The U.S. aims to limit China's influence in the Middle East while exerting pressure on Iran as it does not want Iran to become a regional power.

China's policy towards U.S.:

China's policy towards United states has moved from defensive to both offensive and defensive realism. Farhadi and Zhao (2024) China's strategy emphasizes maximizing economic benefits and minimizing commitments in the region, while incrementally seeking to make strategic gains, bolster China's regional and global profile, and challenge American predominance. The key elements of China's policy towards US and its implication on the gulf states include state-led technological advancement such as "Made in China 2025" focusing on high-tech sectors like robotics, aerospace, and renewable energy, and "Belt and Road Initiative" which focuses on connectivity and trade. China's policy towards the United States has been one of strategic competition, with both nations vying for influence on the global stage. This dynamic has significant implications for other countries, including Iran.

China has been strengthening its ties with Iran, particularly in the economic and energy sectors. This partnership is part of China's larger plan to secure energy supplies and reinforce its influence in the Middle East. China's interest in investing in the infrastructural development of Iran and its energy sectors ensures a steady supply of oil and gas flows into its port. It also keeps China strategically sited in an important geopolitical region. The relationship between China and Iran is filled with meaningful implications for both nations and for the international system at large. Equally stressed economically, the Iranian economy has been seething under the pressures of successive U.S. sanctions which is why China's investments in Iran provide crucial support to the Iranian economy (The International Institute for Strategic Studies, 2021, December). These investments not only inject much-needed capital but also facilitate the transfer of advanced technology, helping Iran modernize key sectors such as telecommunications and energy. Geopolitically, the China-Iran relationship is a kind of geopolitical balancing against the role of the U.S. and its allies in the Middle East. Through improved relations with Tehran, China will

expand its international influence in an area that the U.S. has dominated for a long period. Another motive behind this strategic partnership is energy security. Beijing continues to invest further in Iran's energy sector-in oil and natural gas infrastructure, for instance ensure a steady supply of energy supplies other than those from potentially less reliable sources. Thus, this mutually beneficial relationship underscores the broader geopolitical shifts that are all part and parcel of the Sino-U.S. rivalry, with Iran as an emerging pivot player in the contest for regional and global power. Overall, China's policy towards the United States and its growing relationship with Iran are reshaping the geopolitical landscape with potential consequences for regional stability and global energy markets.

China emphasizes the integration of artificial intelligence and advanced technologies in defense, seeking to strengthen its security cooperation with Iran, thereby fostering stability and undermining U.S. influence through diplomatic and economic instruments. China has high-level diplomatic visits, trade agreements, and participation in regional forums with the Gulf states to strengthen ties, promote mutual interests, and counter US pressure and influence.

Future impact of the current situation:

The future impact of the current Sino-US rivalry on Iran brings a complex interplay of opportunities and complexities for the state. The ongoing Sino-US rivalry is likely to have significant future impacts on Iran, shaping its economic, political, and security landscape. The deepening ties between China and Iran have substantial economic, political, security, and global implications. China is giving Iran an economic lifeline in the infrastructures, energy, and technological areas since international sanctions crippled the economy of this country. Economic ties are even stronger with improvements in trade relationships through China's ongoing imports of oil and gas from Iran, as well as exchange for products and technology. Politically, the 25-year Comprehensive Strategic Partnership between the two nations enables them to counterbalance U.S. influence in the region, while Iran's alignment with China could shift the power dynamics in the Middle East, bringing closer ties with players like Russia. On the security front, a formal military alliance is unlikely, but China and Iran are likely to continue holding joint military exercises and strategic cooperation. The U.S. may enhance its military posture and diplomatic engagement in the Middle East in response to Chinese expansionist influence. Globally, Chinese reliance on Iranian energy would influence energy markets, potentially impacting oil prices and supply chains, whereas the Sino-U.S. rivalry in the Middle East will reshape geopolitical dynamics, affecting alliances and international relations. In a nutshell, the Sino-US rivalry is set to greatly influence Iran's future. Both opportunities and challenges are seen to arise from this complex geopolitical landscape. The increased reliance of Iran on Chinese technology is reshaping its digital and geopolitical landscape but brings with it both opportunities and challenges. As US sanctions limit access to Western technologies, dependence on Chinese telecommunications and digital infrastructure is expected to grow and make Iran a more integral part of the technological ecosystem in China. While this arrangement creates short-term solutions, it makes Iran an increasingly vulnerable hostage to Beijing's strategic priorities, which might also work against diversification of its technological base in the long run. With China's backing, Iran will also increase its native cyber power, becoming a regional cyber leader. This would, however, make the situation more tense in the region, particularly with Israel and the GCC states, which have aligned themselves with U.S. cyber strategies. Meanwhile, U.S.-led efforts to isolate Iran technologically may push Tehran out of global tech standards and innovation and deepen its dependence on Chinese systems. This technological fragmentation could slow Iran's access to cutting-edge

advancements, leaving it dependent on Chinese innovations, which in some cases may lag behind their Western counterparts.

Main Body:

The Sino-U.S. rivalry cuts across multiple domains, and cyberspace has emerged as a critical battleground. Iran has a very strategic geopolitical position and a contentious relationship with the US, which is why it is perceived to be increasingly influenced by both superpowers. From China's Digital Silk Road initiative to the US's cyber containment strategies, the Sino-US competition has deep implications for Iran's technological infrastructure, security policies, and global alignment.

Sino-US rivalry on cyberspace:

The United States has long been trying to continue its pinnacle of dominance in global cyberspace through an open and interoperable internet and by using its technology and economic power against adversaries. This dual stance of the US towards Iran attempts to constrain Tehran's cybersecurity and technological capabilities. Sanctions and prohibitions are opened to the United States for its capability to inhibit Iran's further acquisition of cutting-edge technical technology produced or modified in the West, high-level digital edge architecture, and cyberspace tools. The US can encourage further stagnation of Iran's technological power as the rest of the world advances to more substantial integration in the digital economy. Moreover, due to the protracted cyber offensive that shaped Washington into one of the strongest weapons in the sphere of international strategy, a situation of sabotage activities like Stunt has been appropriately taken up by the US as a method of strategic intervention into Iran's nuclear affairs. US cyber sabotage actions are not only aimed at disrupting Iran's military and nuclear progress but also at sending a very clear message to others that the US has potent offensive cyber capability. By isolating Iran from global digital ecosystems and impeding its technological growth, the US strategy is meant to undercut Iran's ambitions and mitigate its influence.

Unlike the US, China conceives of ascending cyberspace through initiatives such as the Digital Silk Road, that provide an alternative digital ecosystem aligned with Chinese political and economic interests. As far as cooperation with Iran is concerned, China is one of the largest providers of telecommunications infrastructure through advanced technologies such as 5G. This helps Tehran circumvent the technological barriers imposed by the US and modernize its communication systems hungry for improvement, yet in line with its connectivity to the digital universe. China also provides Iran with cybersecurity capabilities and resources and telecommunication aid to help the latter mitigate the overreaches of US sanctions, especially on Iranian cyber and military programs. Observing this, however, we cannot help but see that Iran, in fact, stands at a very complex position in the interplay of the Sino-American cyberspace rivalry, acting both as a benefactor and one of the global war fronts. On the one hand, Iran benefits a lot from its ever-growing dependence on Chinese technology to help it bypass US sanctions and build up adequate cyber and technical capabilities. This cooperation, however, strengthens Iran's technological independence also because it would be in closer alignment with China's ordering vision of a multipolar world. Its geopolitical position is complicated on the other hand owing to another factor which has to do with Iran being opposed to the US; that is, Iran finds itself of a different opinion from Washington with regard to regional and global strategy. With its improvement in cyber capabilities with the help of China, Iran is drawn further into the loosely configured Beijing-dominated order by aligning its interests with China's challenge to US domination. At the same time, Iran's own acts-such as cyberattacks against regional opponents like Israel or Saudi Arabia-reflect a quest for strategic autonomy against mounting external pressures.

Theoretical Framework

The research aims to use the theory of Neo-realism or Structural realism given by Kenneth Waltz in 1979 as well as Security Dilemma given by John H. in the 19th century, focusing on the pursuit of power and security, anarchic structure of cyberspace and bipolar distribution of power. The nature of the international system is defined by its ordering sole principle which is 'Anarchy'. Every State is independent in this system and wants to ensure its survival. This brings mistrust and fear among states and makes them pursue their interests rather than fulfilling others. This explains the competitive and influencing behavior of the US and China towards Iran to pursue their interests and fulfill their energy or domination goals in the region. The growing uncertainty and fear in Iran relations is also due to the structure of the International System and the role of two leading powers of the world; US and China. Hence the theories of neorealism and security dilemma are used in the theoretical framework as structure is the main reason that despite being influenced by the US and China the relations with Iran exacerbate rivalry and mistrust rather than cooperation.

Theoretical frameworks such as neo-realism, security dilemma, and constructivism offer critical insights into the implications of the Sino-US rivalry in cyberspace for Iran's positioning and strategy. These theories illuminate how systemic pressures, perceptions of security, and ideational factors shape Iran's behavior in response to global competition.

Neorealism and balance of power:

Neorealism, a theory that emphasizes the anarchic nature of the international system, survival as the highest security end, and the importance of power maximization for states, provides a lens through which we understand Iran's behavior in the Sino-US rivalry (Waltz, 2014). Neo-realism suggests that the anarchic international system compels states to maximize their power to ensure survival, often forming alliances with stronger states to counterbalance systemic threats. Iran, as a secondary power in the global order, faces a difficult position between two major powers: The United States, the current hegemon, and China, the rising power. In response to US hegemony and its increasing pressure through sanctions and cyber operations, Iran has aligned itself with China. Iran views the global competition between the United States and China as an opportunity to strengthen its own security and technological capabilities while navigating systemic pressures. As a secondary power, Iran has no choice but to align with one of the great powers to survive and expand its influence in an integrated cyberspace. By embracing China's technological assistance, Iran increases its relative power in cyberspace, offsetting its vulnerability to US sanctions and cyber operations. This alignment allows Iran to counterbalance US dominance and solidify its position in a rapidly evolving digital ecosystem. Neo-realism highlights how Iran's strategic calculus revolves around utilizing the Sino-U.S. competition to secure its place in the international system.

Security Dilemma:

The security dilemma explains how one state's efforts to enhance its security through military or technological advancements are perceived as a threat by other states, prompting them to take countermeasures that ultimately increase tensions and lead to an armed race. Iran views its growing cyber capabilities which are developed with Chinese assistance, as defensive measures against the US's hostile actions, including sanctions and cyber offensives. Iran's regional rivals, such as Israel, Saudi Arabia, and the UAE, see these actions as threatening, believing that an expanding Iranian cyber arsenal is offensive. These states invest much in their own cyber defenses, often with US assistance, which produces a regional cyber arms race. For example, Iranian cyberattacks on Saudi oil facilities or Israeli infrastructure invariably trigger retaliation, thus

fueling regional tensions. The competition between the US and China intensifies this security dilemma, and each power's actions in cyberspace indirectly deepen Tehran's perceived vulnerability, thus causing it to further enhance its cyber capabilities. This only drives insecurity deeper, perpetuating an unstable and conflict-prone environment in cyberspace. Tehran views the advance of its cyber capabilities, given substantial Chinese material input, as a necessary defensive effort meant to protect Iranian interests and legally avoid US- imposed sanctions and cyberattacks.

Countries like Israel, Saudi Arabia, and the UAE see Iran's growing cyber power as a threat, so they're beefing up their own cyber defenses, often with help from the U.S. This has led to a regional cyber arms race, where every time Iran makes a move, like launching a cyberattack on Israeli or Saudi targets, it sparks retaliation, making the whole region more unstable. On the global stage, the rivalry between the U.S. and China makes things even trickier for Iran. While the U.S. tries to slow down Iran's cyber growth with sanctions and attacks, China's support helps Iran boost its cyber capabilities, making it harder for the U.S. to stop them. As Iran works to strengthen its position, it only increases fears and tensions with other countries, keeping the cycle of instability going in cyberspace.

Constructivism and cyber-norms:

Constructivism emphasizes the role that ideas, norms, and identity play in the behavior of states. Unlike materialist theories that base their reasoning more on material interests, constructivism postulates that international relations are formed based on collective ideas and values that define what states should act upon. Iran's alignment with China reflects ideological affinity, such as on issues of "cyber sovereignty," which emphasizes state control of digital spaces and national data. It contrasts with a US-led view of a free, open, and interoperable internet. Iran's embrace of China's cyber norms is driven not just by practical interests but also ideological affinity; both express skepticism about US dominance in cyberspace. As Iran endorses China's position in forums outside the Western fold, such as the United Nations, it further develops a fragmented cyber order and a mutually contested norm of internet governance. Iran's actions in cyberspace thus reflect both a resistance to US power and the ambition to shape the global cyber governance per its vision. Through this ideological alignment with China, Iran becomes a powerful tool in the contestation over cyber norms, countering the US-led liberal order and accentuating closer state control over cyberspace.

Conclusion

Theoretical frameworks reveal the deeper systemic, regional, and ideational implications of the Sino-US rivalry for Iran. Neo-realism and offensive realism emphasize the pressures of the system and the quest for power maximization, while the security dilemma reflects unintended consequences stemming from the defensive state measures; these include irrationalities based mainly on fear when deploying the security issue. From these theories, Constructivism points to how Iran is integrating its norms with that of China, whereas dependency theory places Iran on caution so as not to be overly dependent on Beijing. Together, these theories serve as evidence for the fact that Iran's role in the Sino-U.S. rivalry in cyberspace is a two-edged sword that not only provides it with an opportunity but also a threat, one which transforms it drastically in its future.

Objective:

The objective of this research on "Sino-US Rivalry: Expansion of Cyberspace Influence on Iran" would be multifaceted, aiming to explore the geopolitical, strategic, and theoretical dimensions of this issue. Below are the key objectives:

Sino-US rivalry in cyberspace has become an essential part of global geopolitics and has spread into different regions, including the Middle East. This competition between the United States and China in the cyber domain is not only about supremacy in technology but also about forming global governance and winning influence over strategic partners, of which Iran is a key player in this rivalry. The U.S. and China use different tools, policies, and technologies to project their cyber dominance. While the U.S. exerts influence over Iran's digital infrastructure and denies access to advanced technologies, China extends technological partnerships with Iran that can enable it to build and strengthen its own cyber capabilities, such as cybersecurity tools and surveillance technologies. These interactions go a long way to shape Iran's cybersecurity landscape since China's influence opens up Iran's opportunities of building a robust digital infrastructure but US cyberattacks and sanctions undermine this.

By aligning itself with China, Iran finds a source for technological resources against the sanctions and cyber pressure exercised by the United States. Of course, all these alliances entail risks, namely that excessive reliance on Chinese technology might expose the Iranian side to future vulnerabilities of its cyber defenses. The broad regional implications are also significant within the Sino-US cyber rivalry. With Iranian growing cyber capabilities facilitated by the help of China, the regional power balance could go out of its way and rise tensions with added security dilemmas. The United Arab Emirates and Saudi Arabia have already been troubled by Iran's regional ambitions. They could potentially increase their own cyber capabilities that might create a cyber-arms race. Furthermore, Israel, as a regional power with developed cyber capabilities, may also be attracted into this cyber competition and thereby further inflate regional instability.

The rivalry between the US and China has a very important implication in the global context of cyber governance. Iran's support for China on issues like "cyber sovereignty" supports the Chinese vision of a decentralized internet where each state exercises control over its digital infrastructure. This is against the US vision of a more open and global internet governance model. As Iran aligns itself with China, it may contribute to the fragmentation of global cyber norms, with regional actors like Iran, China, and Russia pushing for a cyber-governance model that reflects their preferences and values. This shift could further complicate global efforts to establish cohesive cybersecurity standards and norms.

The long-term risks and opportunities for Iran in this context are multi-dimensional. On one hand, over-reliance on Chinese technology could expose Iran to potential vulnerabilities, as the US could exploit its dependence on Chinese infrastructure in future cyber operations. On the contrary, the tie up with China provides Iran with a strategic opportunity of self-improving its technical power and reducing its technological reliance on Western elements, since all these capabilities had been considerably impaired by sanctionable measures against Tehran. Further, this coalescence also likely to present opportunities for gaining even more substantial shares in worldwide deliberations for regulating the Internet cyberspace - precisely because it increasingly becomes one arena of rivalry.

This triangle is also quite challenging for the policymakers of Iran, China, and the US. Iran has to balance its dependence on China with managing risks from US cyber offensives. China and the US, the two super cyber powers, need to reduce the risks of an escalatory spiral and find ways to promote cooperation in the field of cybersecurity to maintain stability in the region and world at large. The reduction of cyber tensions and strengthening of stability would thus be furthered by way of diplomacy, trust-building, and cybersecurity arrangements.

The research provides a comprehensive understanding of the Sino-US rivalry's cyberspace dimension and its implications for Iran, giving both theoretical insights and practical recommendations for managing the evolving cyber-geopolitical landscape.

Case Studies:

Case Study: Huawei and the Expansion of China's Digital Influence in Iran

One of the most prominent examples of Sino-US rivalry manifesting in cyberspace influence on Iran involves Huawei, a Chinese telecommunications giant. Huawei's role in building Iran's digital infrastructure underscores how China leverages its technological expertise to deepen ties with Iran, while simultaneously challenging US efforts to isolate Tehran and maintain dominance in global cyberspace.

Background

In 2021, the China-Iran 25-Year Comprehensive Strategic Partnership was formally announced, encompassing areas such as energy, trade, and technology. Central to this agreement was the expansion of Iran's telecommunications and digital infrastructure, with significant contributions from Chinese companies like Huawei.

This partnership became an issue in the rivalry of Sino-US during US escalation sanctions on Iran and limit global operations of Huawei because of security concerns. The US claimed that Huawei technology can be utilized for espionage and cyber activities while China presented itself as a trustworthy partner for Iran, providing critical digital tools against American pressure.

The partnership between Huawei and Iran is a critical development in terms of technology, geopolitics, and the global balance of power. Huawei has been instrumental in transforming Iran's telecom infrastructure, leading 5G rollouts in several cities by 2023 and upgrading legacy 3G and 4G networks. This has effectively made Iran an isolated leader in digital connectivity among sanctions on its access to Western technologies. Huawei's involvement also extended to cybersecurity and surveillance, providing Iran with tools like facial recognition, internet monitoring systems, and encrypted communication platforms. These technologies have not only quelled Iran's grip on digital communications but were reportedly used to stifle domestic dissent during protests in 2022 and 2023, reflecting a shared emphasis between Iran and China on "cyber sovereignty" (Vaisi, 2022). Huawei connected Iran to China's Digital Silk Road as part of the Belt and Road Initiative, helping Iran move toward a digital economy by improving areas like digital payments, e-commerce, and cloud services. While this brought innovation and new opportunities for Iran, it also deepened the country's reliance on Chinese technology, sparking concerns about how much control and influence China might gain over Iran's systems.

The US responded aggressively to the Huawei-Iran collaboration, imposing secondary sanctions on Iranian entities partnering with Huawei and accusing the company of facilitating espionage. In 2022 and 2023, the US escalated its countermeasures by launching cyber operations targeting Iranian infrastructure dependent on Huawei equipment and strengthening cybersecurity alliances with GCC states to counter Iran's growing cyber capabilities. These efforts aimed to curb Huawei's influence while reinforcing US-aligned digital infrastructure in the region (Mulligen et al., 2021).

However, there is more to it than meets the eye. Huawei's assistance to Iran enabled its technology and strategic gains, allowing it to circumvent sanctions and modernize its telecommunications. However, it further increased Iran's dependence on Chinese technology, leading to fears of external domination. For China, Huawei's interventions increased Beijing's influence in the Middle East--the very epicenter of US geopolitical interests--to serve as a tool against US dominance in the

global arena. Accordingly, in the light of this prospect, the partnership revealed the obsolescence of the use of sanctions and showed how the scope for stopping China's growing cyber influence has become more difficult, witnessing a rise in tensions between Beijing and Tehran. The Huawei-Iran partnership can also be studied through multiple theoretical lenses. In particular, the neo-realist theory projects a balance-of-power paradigm, wherein Iran is aligning with Beijing to resist any likely pressures from the US and, in turn, Leverage on Iran was for a foothold into the Middle East-an easier pasture. The security dilemma plays out as Huawei's expansion into Iran was viewed by Tehran as purely defensive, therefore escalating tension in the region with the US and its allies, leading to counter-reactions. Dependency theory illustrates the increasing dependence of Iran on Chinese technology and brings vulnerabilities into different asymmetric partnerships. Finally, constructivism clarifies the ideological undertones connecting Iran and China, with Huawei's action reinforcing the Chinese perception of "cyber sovereignty" as a viable alternative to the US-popularized version of an open internet. This partnership thus reflects the nexus of technology and geopolitics in the transformation of the power politics sighting in the Middle East.

Case Study: Stuxnet, Its Aftermath, and the Sino-US Cyber Rivalry in Iran

While the Stuxnet attack (discovered in 2010) predates the current period of intensified Sino-US rivalry, its aftermath continues to shape the dynamics of cyber influence in Iran. The incident not only escalated Iran's focus on cyber capabilities but also positioned Iran as a contested space for great-power cyber influence, particularly in the Sino-US rivalry from 2021 to 2024.

Background

Stuxnet, a computer worm, which is said to have been designed by the U.S. and Israel, was reported to have attacked Iran's nuclear centrifuges and caused major damage to its nuclear program. This cyber-attack was a game-changer in the world of cyber warfare and had a significant influence on how Iran approaches its cybersecurity.

After the attack, Iran started investing heavily in cyber capabilities as part of its national defense strategy. In this context, which surfaced between 2021 and 2024, China had fertile ground to step into as a strategic partner, countering US influence and helping Iran develop its cyber defense, while the US was looking at curtailing Iranian cyber activities and Chinese involvement.

Dastardly developments following the Stuxnet cyberattack emphasize the increasingly central role that cyberspace now plays in rivalries between Washington and Beijing because Iran has lately taken center stage in the increasingly sharp geopolitical standoff. After Stuxnet unmasked vulnerabilities in Iran's critical infrastructure, the country began attempts to boost its cyber defenses, turning to China as a major partner in their 25-year comprehensive strategic partnership. Chinese firms transferred advanced cybersecurity technologies such as firewalls, malware detection systems, and encryption capabilities to Iran. Joint research by Chinese and Iranian experts was also undertaken to produce indigenous solutions, which would help Iran reduce its reliance on the West. Learning from its own situation regarding US cyber surveillance, China provided Iran with strategic insights to help strengthen its defenses and allow it to better protect its critical infrastructure. The Stuxnet incident and its aftermath catalyzed a cybersecurity arms race, intensifying the Sino-US rivalry. China leveraged its partnership with Iran to expand its influence through initiatives like the Digital Silk Road, integrating Iran into its cyber ecosystem. In contrast, the US viewed Iran as a testing ground for countering Chinese cyber strategies, resulting in an escalation of offensive operations against Chinese-built systems in Iran. This dynamic has deepened the regional security dilemma, as Iran's enhanced cyber capabilities have alarmed neighboring states like Saudi Arabia and Israel, prompting them to strengthen their

defenses and retaliatory capabilities. China's involvement has added complexity to this regional competition, with Gulf states perceiving it as a strategic challenge to their US-backed security frameworks.

Globally, the Stuxnet case underscored the absence of norms governing cyber warfare. The Sino-US rivalry has further fragmented any efforts to establish such norms, with Iran aligning with China's vision of cyber sovereignty and opposing US-led initiatives for an open and interoperable internet. This ideological divide reflects the broader fragmentation of cyberspace, with competing visions of state control versus openness shaping global cyber governance.

Theoretical insights drawn from this case suggest several dynamics. Neo-realism explains the anarchic nature of cyberspace, wherein states like Iran align themselves with stronger powers like China to counterbalance US dominance. The security dilemma is evident in how offensive cyber operations by the US prompted Iran to enhance its capabilities, thereby causing the situation to escalate further. Framing cyberspace as a battlefield, Stuxnet reinforced the narratives of resistance in Iran and justified its cyber alignment with China. In general, the case demonstrates how Iran has become a testing ground for broader cyber strategies, risks of dependency on Chinese technology, and growing fragmentation of cyberspace along geopolitical lines.

The legacy of Stuxnet continues to shape the dynamics of Sino-US rivalry in cyberspace, with Iran at the epicenter of this geopolitical contest. The case is an example of how cyber incidents can redefine international relations, compelling states to re-evaluate their alliances, strategies, and capabilities. Because of the Sino-US rivalry, Iran's cyber domain remains an important flashpoint of the implications of great-power competition in the digital age.

Scholarly work:

Numerous scholars and authors have worked on this topic and have given their point of view regarding it:

Rita Parsi: She observes how Iran's fast-growing reliance on Chinese technology may be practical, risky, and mirrors a whole new dimension of geopolitics of the Middle East. The pivot to China is being mainly enforced in the sense that Iran has had no choice but to fight off the physically damaging effect of US-led sanctions that seem to have become the means for isolating the country from both Western markets and technology; it can capture with China state-of-the-art telecommunication, surveillance, energy infrastructure, and trading opportunities to fortify its economy. However, this intensified dependency is a perilous move. In the regional sense, alignment with China may make the relations within the Middle East even more complicated, raising pressures with the Western-aligned countries of Saudi Arabia and Israel. Parsi's analysis underscores how Iran must tread a balance between immediate economic and technological gains from Chinese assistance and the long-term benefits to its autonomy and strategic geopolitical posture.

Hooman Peimani: The Iranian government claims that it is through the strategic alliance between the cyber forces of Iran and China that it has been able to break itself out of technological isolation, particularly under the previous US sanctions and global restrictions. These partnerships have allowed Iran to access advanced technologies in areas such as cybersecurity, telecommunications, and digital infrastructure, enabling the country to modernize key sectors despite its isolation from Western markets. By aligning with China, Iran also gains a strong ally to strengthen its determination against external pressures (Peimani, 2017). However, Peimani argues that the reliance on a single partner, especially if that partner is as powerful as China, may pose a threat to Iran's independence in the long term. It stands the risk of becoming indoctrinated into the use of

Chinese technology and expertise and, therefore, losing the adequate ability to navigate its technological and strategic future independently as vital systems and infrastructure get intertwined with Chinese interests. This would end up being an unequal relationship where Iran surrenders to its sovereignty and a pivot away from China turns out to be a herculean matter should new geopolitical conditions arise.

Valerie Hudson: Iran's partnership with China, he argues, is fully rooted in the more sweeping geopolitical strategies that are bent on countering US hegemony and maintaining Iran's regional influence. By building an advanced partnership with China, Iran will procure critical technology, infrastructure, and economic support to buck the pressures of US sanctions and avoid complete diplomatic isolation. In effect, it grants protection for Iran: the country will gain a robust global partner, which counters US moves, whilst making Tehran independent of Western systems. Coincidentally, Iran seeks to use its relationship with its Asian counterpart to sustain and even grow its powerful influence in the Middle East, which gives it a somewhat powerful identity to withstand external pressures. But Hudson also cautions that such alignment does present complications. Iran is also charged with ensuring the partnership does not over-rely on China, as that would further undermine Iran's autonomy and bargaining chip in the region. The partnership is, therefore, seen by Iran as fitting with its wider strategy of attempting to gain leverage on a world stage and the region, in resisting Western encroachment.

Recent Developments (2021–2024)

- In response, the Biden administration conducted military strikes against Iranian targets in Yemen, Syria, and Iraq after a drone attack by Iranian-backed militants led to the death of three U.S. service members. Sanctions were also imposed, and indictments were made against members of the IRGC. Reports also suggest the U.S. carried out cyber operations targeting Iran. The intention of President Biden was to convey a strong message to Iran that he has been feeling domestic political pressure due to the election year and pressure from some Republicans for a strong and direct response against the Iranian government, using long-range bombers to display U.S. military power with a little originality that seeks to deter a future attack.
- Amnesty International. (2024, March 6) concluded that Iran is using AI to enforce strict dress codes and suppress dissent, especially targeting women who violate hijab laws. Proposed legislation includes AI-powered facial recognition to monitor and penalize non-compliance, with over a million women already warned about potential car seizures. Under the Chinese support, Iran has been able to bring facial recognition technology on board, in 2022, to widen the coverages of surveillance. Hence, this technology not only keeps a tab on women but also dissidents and examines digital activities to facilitate a more efficient process of censorship in scopes. It prevents the opposition from organizing and strengthening the regime's control. Iran uses AI in conducting cyberattacks and disinformation campaigns targeting the U.S., Israel, and others. By merging AI with surveillance and cyber tactics, Iran is solidifying its internal control, challenging adversaries in the global landscape. What might this portend for the future of Tehran with respect to its cyberspace and information contexts? And does Iran have the wherewithal to charge ahead with their AI?
- In the beginning of this year, the Institute for Security and Technology did publish that Iran has started to apply AI with the support of China and Russia to increase its cyber-attacks and issued a report on the malicious use of AI envisioning several possibilities conforming to Iran's historical pattern of behavior and supposed intentions. While Iran might be limited in its capabilities in certain areas involving AI development, the collaborations with China and Russia present vast opportunities to develop and weaponize state-of-the-art technologies such

as AI. Also, Iran employs AI as a mode of both undermining the U.S. and its allies while also striving for better positioning in the global tech race with regard to regional competition. Iranian state actors have already started integrating several touchpoints into the operational activities, whereby such touchpoints include the capability to surpass language barriers, automatically generate realistic content, and identify and select potential targets from pools. Recently, Iranian activities are demonstrating the melding of this combination of factors. Open-AI reported that hackers linked to Iran, amongst others from China, North Korea, and Russia, utilized Chat-GPT in three incidences of cyber operations in 2024. For instance, the Iranian group known as "Crimson Sandstorm" used Chat-GPT to create phishing emails, including fake messages from international agencies, improving the English content therein for coercive operations. Open-AI went on to detail in May and August 2024 how these Iranian actors used AI to strengthen deception campaigns in both their cyber and information operations.

- In March 2023, Michael Doran argued that America's unwillingness to form an anti-Iran alliance is essentially handing the Middle East over to China. While China isn't directly involved in Iran's aggression against U.S. allies, Chinese President Xi Jinping is strengthening ties with Iran to secure energy resources and win favor with oil-rich Gulf states. As long as the U.S. avoids taking a stronger military stance against Iran or offering a solid alternative to China's promises, the partnership between China and Iran will keep growing, along with their influence in the Middle East.

China is strengthening its partnership with Iran by purchasing an increasing amount of oil and helping Tehran evade sanctions.

- China buys most of Iran's illegal oil exports and helps Iran bypass sanctions by using Chinese banks for oil payments and other restricted transactions.
- Suspicious oil imports from Malaysia: In December 2022, China reported importing unusually high amounts of "Malaysian oil." Experts believe much of this oil is actually Iranian oil being disguised as Malaysian.
- Iran uses a "ghost fleet" of tankers to secretly move oil, registering them in countries like Panama, Liberia, and the Marshall Islands. The U.S. could work with these countries to close this loophole (Hudson institute, 2024 October 9).

Conclusion

The expansion of Sino-US rivalry in cyberspace profoundly shapes Iran's technological, economic, and security landscape. Although Tehran has clearly been benefiting from these rivalries in countries, the growing dependence on China has brought new challenges for Tehran in terms of its autonomy and the continued stability of the region. In turn, the fact that cyberspace has turned into a highly contested domain makes Iran's strategies highly influential concerning shaping its position in the global order as well as the broader Middle Eastern geopolitical climate. The U.S. has been trying to pressure the Iranian tech scene by slapping sanctions on Iranian companies to prevent them from accessing advanced technology. Meanwhile, they have been collaborating with countries like Israel and Gulf states to increase defenses against any potential cyberattack from Iran. In addition, the U.S. has also undertaken cyber assaults against Iran to disrupt Tehran's military and nuclear endeavors to stall technological progress. At its peak, China will become a very vital player in the development of Iran's tech options, especially 5G networks, providing insights toward bolstering Iran's impression against cyberattacks. Colorful rhetoric aside, the economic ties between Beijing and Tehran have entered a broader vista: on a day-to-day basis, Chinese companies are forming part and parcel of Iran's digital economy. This makes Iran all the more dependent on China, particularly for growth opportunities in the technological arena,

aligning Tehran's future for technological developments more squarely on China's grander global vision.

Iran is increasingly becoming reliant on reliance on the digital systems created by China, which has its advantages to Iran's tech scene in the short term, but with some risks attached.

By depending on China, Iran could be giving Beijing the power to spy on or control its digital policies, making the country more vulnerable in the long run. While the Chinese investment is good for Iran's economy right now, it also ties the country closer to China's geopolitical goals, making it harder for Iran to make deals with other countries, especially the West. As Iran builds up its cyber power with China's help, it's only increasing tensions in the region with countries like Israel and Saudi Arabia, who see it as a threat. This could lead to more cyber conflicts and make Iran a bigger focus of regional security issues. Finally, by aligning with China, Iran is supporting a different approach to the internet, one that focuses on "cyber sovereignty" instead of a free and open internet. This goes against the U.S.-led model and pushes Iran to advocate for this new vision in international forums.

As tensions between the U.S. and China continue to grow, Iran is likely to become a major cyber player in the region, which could lead to more conflicts with its neighbors. With more countries ramping up their cyber capabilities, we can expect to see more cyberattacks and counterattacks, making the security situation even more challenging for everyone involved. Iran's closer ties with China will pull it further into Beijing's vision of a divided internet, moving away from Western ideals and contributing to a more fragmented cyberspace. This shift could create competing zones of influence online. For China, having influence over Iran's technology gives it significant leverage, allowing China to guide Iran's decisions, especially in its ongoing rivalry with the U.S. China could use Iran as a strategic piece in its broader cyber and geopolitical strategy.

References

- Amnesty International. (2024, March 6). Iran: *Draconian campaign to enforce compulsory veiling laws through surveillance and mass car confiscations*. Iran: Draconian campaign to enforce compulsory veiling laws through surveillance and mass car confiscations - Amnesty International
- Baycar, H. (2023). *China-U.S. Rivalry Enters a New Phase in the Middle East*. Washington: Carnegie endowment for International peace.
- Farhadi, A., & J., A. (2021). *The Great Power Competition Volume 1*. Switzerland: springer.
- Farhadi, M., & Zhao, L. (2024). Exploring the Impact of Iran-China Trade on Environmental Sustainability. *Journal of Energy and Environmental Policy Options*, 7(1), 1-8.
- Freddy, H. J., & Bijukumar, V. (2024). Case Study I: US-China Rivalries. In *New Trends in Emerging Power-Great Power Conflicts* (pp. 37-62). Cham: Springer Nature Switzerland.
- Hudson institute. (2024, October 9). China-Iran Relations in the Rising Axis.
- Kuo, M. A. (2022). The Gulf States in China-US rivalry. *The Diplomat*.
- (2021). *Relation between China and the Arab Gulf states*. Bahrain: IISS.
- Mulligen, Stephan P., & Linebaugh, chris D., (2021). *Huawei and U.S law*. Congressional Research Service. Huawei and U.S. Law
- Piemani, (2017), China and Iran: Energy Security Cooperation, but not Much More. FA3-maintext2
- The International Institute for Strategic Studies (2021, December). *Relations between China and the Arab Gulf states*. 27, Retrieved from <https://www.iiss.org/publications/strategic-comments/2021/relations-between-china-and-the-arab-gulf-states/>Thomas, C. (2024). *Iran-Supported Groups in the Middle East and U.S. Policy*. Congressional Research Service.
- Waltz, K. N. (1990). Realist Thought and Neorealist Theory. *Journal of International Affairs*, 21-37.
- Waltz, K. N. (2014). Realist thought and neorealist theory. In *The Realism Reader* (pp. 124-128). Routledge.
- Kenneth N Waltz. "Realist Thought and Neorealist Theory." *Journal of International Affairs*, 1990: 21-37. Realist Thought and Neorealist Theory on Jstor
- Kausch, Kristina. (2017, November 24). Cheap Havoc: *How Cyber-Geopolitics Will Destabilize the Middle East*. Cheap Havoc: *How Cyber-Geopolitics Will Destabilize the Middle East* | German Marshall Fund of the United States
- Vaisi, Ghazal. (2022, March 01). The 25-year Iran-China agreement, endangering 2,500 years of heritage. Middle East Institute. *The 25-year Iran-China agreement, endangering 2,500 years of heritage* | Middle East Institute
- Mulligen, Stephan P., & Linebaugh, chris D., (2021), *Huawei and U.S law*. Congressional Research Service. Huawei and U.S. Law
- Reuters, (2021). Iran and China sign 25-year cooperation agreement. Reuters. *Iran and China sign 25-year cooperation agreement* | Reuters

Piemani, (2017), *China and Iran: Energy Security Cooperation, but not Much More*. FA3-maintext2

Amnesty International. (2024, March 6). Iran: Draconian campaign to enforce compulsory veiling laws through surveillance and mass car confiscations. Iran: *Draconian campaign to enforce compulsory veiling laws through surveillance and mass car confiscations* - Amnesty International

Hudson institute. (2024, October 9). *China-Iran Relations in the Rising Axis*.