International Journal of Political Science
ISSN: 2228-6217
Vol 14, No 2, June 2024, (pp. 191-202)

The Role of Cyberspace in the Security Policies of the Chinese Government

Roshanak Ezzati [1], Garineh Keshishyan Siraki[2*], Seyed Mostafa Abtahi[3]

[1]Department of Political Science, Science & Research Branch, Islamic Azad University, Tehran, Iran
[2*]Department of Political Science, South Tehran Branch, Islamic Azad University, Tehran, Iran
[3]Department of Political Science, Science & Research Branch, Islamic Azad University, Tehran, Iran

Received: 15 Feb 2024 ; Accepted: 20 June 2024

Abstract

One of the principal axes of security threats in the era of communications and globalization for states lies in the cyber domain. In response to international developments, specific countries, including China, have concluded that to pursue their objectives and safeguard their interests, they must adapt to the new global environment, seek a novel power, and consolidate a new type of authority, namely, smart power. By acquiring modern technologies, China has sought to counter the security threats that endanger it domestically and internationally. This study examines cyberspace's role and position in shaping China's security policies and seeks to address the question: What is cyberspace's impact on ensuring China's national security? Employing a descriptive-analytical method, the research draws upon library and internet sources and the securitization theory to analyze the issue. The key findings indicate that cyberspace and its role in security are paramount for China, particularly as it aspires to elevate its status from that of a regional power to a global one. Accordingly, China has incorporated soft power instruments and the strategic utilization of cyberspace into its security policies. In the contemporary era, some states, including China, perceive cyberspace as threatening the prevailing political system. The Chinese government has adopted policies centered on surveillance and controlling citizens' information to counter these risks. Furthermore, through comprehensive and multidimensional strategies including stringent legislation, investment in advanced security technologies, and international cooperation in cybersecurity, China has achieved considerable success in mitigating such threats.

Keywords: Cyberspace, Security Policies, Surveillance, Information Security, China

[*]Corresponding Author's Email: g.keshishyan@iau.ir

Introduction

In the present century, internet communications have reached their highest level, and individuals and institutions exploit cyberspace's full range of possibilities to advance their objectives. Technology and digital innovation have consequently emerged as key power sources for states to counter cyber threats. Given the increasing dependence of governments on communication tools, coupled with the frequency and sensitivity of cyberattacks in recent years, cybersecurity has become paramount, particularly for states.

In the communications era, with the transformation of traditional concepts of power and security and new dimensions of threats, attention to the internet and cyberspace has become crucial. It will increasingly remain one of the central pillars of policymaking and decision-making within governments. The rapid advancement of digital technologies and the expansion of cyberspace have significantly altered the global security environment. As one of the world's great powers, China must adapt to these transformations and adjust its security policies in response to the new threats and opportunities emerging from cyberspace.

A review of China's historical integration into the global internet and its activities in the virtual sphere demonstrates a distinctive approach in confronting this modern global phenomenon. This approach has led to policies, structures, and requirements tailored to the challenges of cyberspace. For a country like China, cyberspace is perceived as a threat to the ruling political regime. Chinese authorities consider the absence of control over cyberspace as equivalent to losing their system and sovereignty. This perception has generally resulted in the imposition of filters and restrictions on users' access to the internet. Consequently, the government's primary objective in imposing such limits has been safeguarding information security.

Cyberspace, in turn, demands innovative and forward-looking strategies in national security. Realistically, understanding security threats requires attention to software-based factors, which are the essential link between a state's security environment and hardware infrastructure. Indeed, one of the principal axes of security threats in the era of communications and globalization must be identified in the cyber domain.

The present study seeks to analyze the influence of cyberspace on China's security policy and to address the central research question: What is the impact of cyberspace on China's security policies in the pursuit of national security? The findings suggest that information control and cyber-surveillance constitute core elements of China's security and social strategies, enabling the state to maintain political and social stability. Within this framework, the study focuses on the Chinese government's cybersecurity and information security strategy to counter prevailing threats. To this end, the research adopts a descriptive-analytical method, drawing on relevant library and internet sources, and applies the securitization theory to analyze and synthesize the subject matter.

Research background

Mohammad Razzazan (2024), in a study titled Smart Governance in the Age of Artificial Intelligence: Assessing the Impact of China's Policy on the Emerging Technological Order, demonstrates that China, recognizing the

strategic importance of artificial intelligence, has developed comprehensive frameworks and governance policies aimed not only at enhancing its domestic AI capacities but also at influencing the emerging global technological order in this field.

Mojgan Ghorbani (2022), in her research entitled The Role of Cyber Diplomacy in Expanding China's Global Influence, examines cyber diplomacy within international relations, with particular emphasis on China's practical policies in international organizations and its cooperation with other states.

Mohsen Shariatinia et al. (2019), in a study titled China and International Orders, argue that China's strategic behavior in international politics is far more complex than conventional stereotypes such as "challenger" or "revisionist." They demonstrate that China has acted as a challenger within the hegemonic order, a security seeker in the balance-of-power order, and an order-shaping actor within institutional frameworks.

Shahrouz Ebrahimi et al. (2014), in a study titled China's Defensive-Offensive Approach in Cyberspace, reveal that China, in designing its future warfare strategies against potential rivals, has formulated its cyber and information warfare doctrine to safeguard its critical infrastructure and networks through a defensive approach while simultaneously targeting the disruption of adversaries' vital infrastructures through an offensive strategy.

Jayasakara (2021) examines China's cyber diplomacy under Xi Jinping's presidency, focusing on the president's liberal policies and pursuit of multilateral diplomacy with the United States and the European Union.

Viti Vinchun (2020), in a study titled The Evolution of China's Security Policy: From Deng to Xi, investigates the overall trajectory and development of China's security policies.

Yang (2016) addresses China's security challenges, identifying the country's priorities and policy directions, with a broader focus on domestic and external security issues.

Theoretical Framework

Securitization: Security in the New Era

National security today faces many threats, among which cyber threats stand out as a novel phenomenon that has arisen alongside the development of information technology and the expansion of communications, confronting governments worldwide. This phenomenon is so recent that the consequences it entails for national security have, to a large extent, been neglected. Over the past two decades, a trend has emerged that challenges the conventional approach to security established within the framework of strategic studies during the Cold War. This trend emphasizes the necessity of moving beyond what many perspectives have considered an excessively militarized interpretation of security, and it has been accompanied by the emergence of new security challenges (Clark, 2007, p. 236).

From this perspective, contemporary security threats are no longer limited to the military domain. Issues such as environmental crises, global poverty, migration, and, more recently, cyber threats pose risks to state security that often surpass traditional military threats. The discourse on cyber threats has been heavily shaped by the ongoing information revolution,

stemming from the dynamic dissemination of information and communication technologies that permeate all aspects of human life (Khalili Pour Rokan Abadi, 2012, p. 186).

In light of the foregoing, cybersecurity is generally defined as "protecting critical information infrastructures, processes, and content." The threats in this domain are expanding daily and becoming increasingly complex, directly influencing states' national security. Within the traditional outlook, states emphasized ensuring their survival and securing military defense. However, states today are forced to consider new dimensions of security. Conventional concepts of war, based on attack and defense, have been challenged by the complexities of cyberspace, which evolve at great speed and, in turn, transform conventional understandings of warfare. Cyber threats are asymmetric; thus, launching an attack does not require substantial investments, while defending against such threats demands a comprehensive approach with rising costs. Consequently, national security can no longer be defined exclusively in terms of territorial borders and protecting citizens' lives through military forces. Cybersecurity is therefore directly and inseparably connected to national security.

The so-called Copenhagen School in international relations has most prominently developed the concept of securitization. This theoretical foundation is situated mainly within constructivism and post-structuralism (Beach, 2012, p. 91). With the end of the Cold War and the decline of the bipolar order in the international system, the security indicators have undergone a profound transformation. As the world has become increasingly globalized and the monopoly of states has diminished, along with the reduced dominance of great powers in determining the balance of power and security in its traditional sense, it has gradually lost significance and taken on new meanings.

In reality, both due to the nature of the contemporary era characterized by shifting sources and geographies of power, as well as the presence of diverse actors in the competitive landscape and the strategic foresight of major players such as China, the primary arena of competition in international relations today is no longer centered on military security rivalries as in the Cold War era (Zarif et al., 2017, p. 98). Instead, the security concept has broadened beyond its traditional military shell. This new conception of security is increasingly defined in terms of technology, economy, commerce, and other domains.

Thus, in this new understanding, security is no longer monopolized or dominated by militarization but has expanded into multiple arenas. A state's security is therefore contingent upon all aspects derived from elements of national power. Environmental, economic, political, and territorial security are meaningful and weight-bearing components of this broader security paradigm. At the same time, classical efforts to "securitize" all of these areas often blur with the original notion of securitization, resulting in formulations such as security economics, environmental security, political security, and ultimately territorial security, all manifestations of the expansion of security discourse into diverse sectors.

Cyber Power

From antiquity to the present day, the concept of power has always stood at the center of political thought. However, with the advent of cyberspace and the advancement of digital technologies, it has undergone a profound transformation. This shift has introduced a new form of power, cyber power, which embodies a combination of both the hard and soft elements of national power and has emerged as one of the most crucial sources of power in the twenty-first century.

Through its extensive influence on economic, military, political, social, and cultural domains, cyber power offers unprecedented opportunities for active presence on the global stage, strengthening the foundations of national security and enhancing states' international standing. Both state and non-state actors can employ this form of power, which reflects the full spectrum of national power in its hard and soft dimensions to pursue financial, military, political, ideological, or social objectives in virtual or physical arenas. Consequently, many states regard cyber power as an integral component of national power and a vital factor to be cultivated through improving its indices in cyberspace.

Quell defines cyber power as "the ability to employ cyberspace to create superiority and exert influence across all operational domains and all instruments of power." In his conceptualization, the operational domains correspond to the five areas of power: land, sea, air, space, and cyberspace, while the instruments of power correspond to the four dimensions of diplomacy, information, military capability, and economics.

Sheldon identifies several key features of cyber power:

a) Cyber power is omnipresent and exerts strategic effects absolutely and simultaneously across all domains.

b) unlike land, naval, or air power, cyber power is a complementary tool.

c) Cyber power may remain concealed, a feature Sheldon describes as one of its major attractions for many users, since it can exert global influence without others detecting their role or agency. He further notes its appeal for states, as the capacity to employ cyber power covertly renders the identity and motivations of attackers difficult to ascertain, thereby making it a beautiful instrument for governments and other actors (Mozaffari Nia, 2023, pp. 19-20).

Since 1999, China has sought to compensate for its technological and military shortcomings vis-à-vis the United States. Beyond the realm of hardware and kinetic weaponry, and in light of its vulnerabilities in cyberspace, China has made concerted efforts over the past two decades to strengthen its cyber defense capabilities. The Chinese possess the necessary infrastructure to conduct denial-of-service attacks, and, if required, they can target the integrity of enemy systems in such a way as to undermine confidence in their command-and-control mechanisms. Although China is not the only active player in this domain, it is widely considered a pioneer.

Cyber Threat

Cyber threats refer to events that, either naturally or through human action (deliberate or accidental), affect cyberspace, or incidents that operate through cyberspace or are related in some way. This novel phenomenon has emerged in recent decades, alongside the evolution of information technology and the expansion of global communications through the vast Internet network worldwide. As a result, today the challenge of cyber threats has acquired particular importance and complexity, stemming from its new nature, distinctive characteristics, and unique manifestations.

The number of components of cyber threats: Multiplicity of actors in cyberspace: The low cost of computer technology, widespread internet connectivity, and the ease of creating or acquiring malicious software mean that virtually anyone can enter this domain. These actors include individuals, organized criminal groups, terrorist groups, private companies, and nation-states.

Low entry costs, minimal time requirements, and high operational speed: To conduct a cyberattack, an individual requires only a computer, an internet connection, and limited technical knowledge of cyberspace. Consequently, cyberspace enables the execution of dangerous actions with low cost, within a short timeframe, and at high speed. Of course, more sophisticated cyberattacks demand higher expenses.

Anonymity of actors and lack of traceability: The Internet was designed as a decentralized system, and its users are often unidentified. This anonymity means that some cyberattacks leave no trace. Actors active in cyberspace can, from anywhere in the world, target digital assets within seconds and without warning, leaving neither evidence nor their names behind.

Profound impact: Cyberspace's distinctive nature creates conditions whereby disruptions or interruptions can have disproportionately extensive consequences. Cyberattacks that cause network disruptions may damage property, time, products, production processes, reputation, sensitive information, and even human lives, as they can undermine vital infrastructures and critical systems.

Diminished role of geography: Cyberspace enables instantaneous transmission across the globe. Thus, attackers can transcend their geographical limitations and reach key targets.

Structure of the Internet: The structure of the Internet exposes governments and private companies to uncertainty regarding cyber risks. This uncertainty arises from the technology's complexity and ongoing evolution in supporting vital systems.

Low likelihood of punishment or accountability for criminal actions in cyberspace: The probability of punishment or accountability for cybercriminal activity is low. Consequently, individuals and organizations perceive cyberspace as safer and less risky than alternative non-cyber options (Khalili Pour Rokn Abadi, 2012, p.169).

China's Cyberspace Governance Policies

China's cyberspace governance policies can be categorized into four dimensions: economic and technical, cultural, security, and managerial/legal:

Economic and technical governance: Intense competition between China's industry and businesses and American hardware, software, and service providers; moving towards self-sufficiency in cyberspace infrastructure and technical equipment.

Cultural governance: Extensive research in fundamental and foundational cyberspace technologies; tight competition between Chinese and non-Chinese content within modern media active in China.

Security governance: Reducing dependency on American infrastructure and services.

Managerial and legal governance: Enacting laws to strengthen China's sovereignty in cyberspace; centralized management and regulation of service provision in China's cyberspace; extensive exploitation of cyberspace diplomacy opportunities to expand China's sovereignty and ensure effective oversight of the Chinese cyberspace (Rezapour, 2019, p.19).

China's Cybersecurity-Oriented Policy

A country's values shape cyber policies and closely align with its military strategies and domestic political agendas. In the draft of China's National Cybersecurity Law of 2015, the core objectives included ensuring cybersecurity, protecting cyber sovereignty, safeguarding national security and public interests, defending citizens' rights, and promoting accurate information. China is the target of some of the most extensive cyberattacks worldwide. Vast intelligence, espionage, and ideological organizations actively undermine China's software security, with billions of dollars in public and classified budgets allocated to this struggle (Moeinpour, 2010, pp. 57-85).

The immense power of the Internet is reflected in the Chinese authorities' deep concerns over excessive access to it. While the government recognizes the network's economic development value, since joining the Internet in 1994, China has consistently sought to shield its citizens from information related to political activists. The Beijing government attempted to block access to numerous websites, including those of foreign publications, human rights and democracy organizations, Taiwanese groups, and sexual content. By late 1997, the Chinese regime enacted regulations defining computer-related crimes. These included using the Internet to slander the government, disclose state secrets, or assist separatist movements. Nevertheless, police oversight did not entirely prevent Chinese activists from maintaining online connections (Alberts & Papp, 2009, pp. 138–188).

China's Measures in Countering Cyberattacks

Cybersecurity issues have gradually evolved into an essential infrastructure for all nations, prompting them to build cybersecurity systems. The development and use of information technology networks and the Internet have become fundamental, constituting a "fifth domain" of national sovereignty alongside land, sea, air, and space. Cyberspace is increasingly viewed as the nervous system of states, indispensable for survival and development.

Analysis of CNNIC reports reveals that the Internet exerts growing influence over social stability, economic development, cultural

growth, and broader strategic cyber policies. With the emergence of cyber-attacks, espionage, surveillance, and information leaks, governments are enhancing their cybersecurity defense systems. China, in turn, has introduced significant measures, most notably establishing a nationwide monitoring system by deploying digital technologies. This framework includes several overlapping and complementary programs to build a comprehensive surveillance infrastructure.

China's Social Credit System

The design and implementation of the Social Credit System constitute the central pillar of China's nationwide surveillance architecture. This technical infrastructure integrates various digital technologies to collect and analyze every citizen's data. Historically, China has had long-standing institutions and mechanisms for gathering citizen data, which were reinforced during the communist era through initiatives such as household registration and the centralized archiving of citizens' identity and personal records (Creemers, 2017).

The modern version of the Social Credit System first emerged in 2011, with the aim of financial credit assessment and managing social crises and vulnerabilities, designed by multiple state agencies. It was formally launched in 2014 under the name "National Unified Plan." The transformative factors enabling this development included the widespread adoption of the Internet, the migration of public and private services onto digital infrastructures, the proliferation of social media, search engines, and connected surveillance cameras, alongside the rapid rise of artificial intelligence and big data. These technological advances gave the Chinese state the capacity to progressively build and operate an ambitious, comprehensive, and intelligent monitoring and control system.

According to official narratives, the key goals of the Social Credit System are: engineering responsible citizenship, improving policy implementation, addressing social problems, and preventing social instability (China, State Council, 2014). The system seeks to prevent crimes linked to fraud and breaches of trust while addressing issues such as weak oversight in market operations, violations of intellectual property rights, rent-seeking, and systemic corruption in economic and commercial projects, all of which undermine growth and development. For this reason, the first group targeted by the Social Credit System was businesses, where an enterprise ranking mechanism was introduced to enhance trust in market products and services. However, many scholars emphasize the political dimension of the program, framing it as a tool of political control (Strittmatter, 2020).

Skynet and Sharp Eyes

In 2005, the Chinese government launched a new national security network named Skynet. This project aimed to establish continuous public surveillance over roads, neighborhoods, schools, universities, airports, restaurants, and shopping centers nationwide. Currently, through the Skynet network, Chinese police can connect to multiple databases and, using augmented-reality smart glasses, identify individuals' faces and match them against existing records. This process enables the authorities to track any violations easily.

In addition to Skynet, Chinese officials launched another project called Sharp Eyes, a high-resolution facial recognition surveillance network built upon Skynet (Feldstein, 2021).

The Golden Shield

Online content censorship is one tool governments use to control what their citizens can access. Since 1998, when the Golden Shield Project launched, China has expanded its surveillance capacity. The Golden Shield is a large-scale state initiative to restrict Chinese users' access to the open Internet and implement widespread censorship by blocking vast amounts of online data. The project's primary objective was to maintain a database of all Internet users and employ it to safeguard national security.

The government could suspend Internet users' accounts if they engaged in inappropriate or non-conforming behaviors. Expressions or content deemed to constitute "illegal" material, such as using Western social media platforms like WhatsApp, were also subject to censorship. Furthermore, in response to resistance from Western companies like Google, which refused to comply with extensive censorship demands, the Chinese government replaced them with domestic alternatives such as Baidu, Weibo, WeChat, and Alibaba (Mishra, 2021).

China's Approach within Cyberspace

Today, information warfare and network-based attacks pose serious challenges to national security. By carefully identifying globalization's security opportunities and vulnerabilities, Chinese policymakers have positioned themselves to respond swiftly and effectively to fluid crises in the digital era.

Chinese security strategists recognize that in the highly compressed and complex process of decision-making, informational superiority can be just as critical and decisive as conventional military superiority (Fritz, 2008, p. 38). Chinese strategists are exploring a new form of warfare that centers on acquiring and disseminating information, attacking enemy data, and conducting defensive information operations, achieving information dominance in future battlefields. In such conflicts, an integrated electronic chip inside a computer may prove far more effective and valuable than a ton of uranium.

Indeed, psychological informational operations today have emerged as one of the most effective instruments of victory in warfare, holding a prominent place in states' defense and military policies. Psychological operations have become one of the most decisive aspects of post-Cold War conflicts. In this context, China, an active and pivotal player in the former bipolar world order, the transitional period, and the current international system, has adopted a strategic outlook toward leveraging such operations to enhance its global influence (Amini, 2004, p. 241).

Although China has experienced remarkable economic growth in recent years, it faces significant political challenges. Alongside its rapid economic and military expansion, the People's Republic of China has, for over a decade, sought to elevate its global standing from that of a regional power in East Asia to a world power. To this end, Beijing has strategically

incorporated soft power instruments and the use of cyberspace into its defensive-offensive posture.

Domestically, this has meant strict laws and policies such as employing informants, monitoring and arresting online dissidents, dismantling physical network infrastructure, and blocking specific websites to suppress dissenting voices. Internationally, China is actively working to expand its advanced cyber capabilities to strengthen its position within the global community.

Investment in Emerging Security Technologies

Since 1999, China has sought to compensate for its technological and military shortcomings compared to the United States. In addition to advancements in hardware and kinetic weaponry, and in light of its vulnerabilities in cyberspace, China has endeavored over the past two decades to enhance its cyber defense capabilities. The scope and nature of its activities indicate that China is preparing to wage future wars through the electromagnetic domain as well as through strategies aimed at denying adversarial access. Chinese strategists recognize the extent of the West's dependence on information technology infrastructures and target this critical vulnerability. They are currently engaged in reconnaissance activities and are expected to leverage this intelligence to secure a strategic advantage in the future. China already possesses the infrastructure to conduct denial-of-service (DoS) attacks. If required, it can compromise the integrity of adversarial systems to such an extent that they lose confidence in their command-and-control networks. While China is not the only state active in this field, it is regarded as a pioneering power.

International Cooperation in Cybersecurity

China has recognized that cybersecurity challenges, including hacking and cybercrime, have evolved into a global concern. Therefore, it acknowledges that only international cooperation can prevent cybercrime and ensure the healthy growth of cyberspace and the internet. From the Chinese perspective, states must cooperate in this realm. All nations should have the right to voice their perspectives, yet they must also shoulder their responsibilities. China maintains that through honest communication and exchanges, the international community will be able to develop effective strategies to confront cyber threats. The country has consistently supported the secure and peaceful use of global information space, while insisting on preserving its national sovereignty and information security (Nagorski, 2010, p. 2).

For many years, China has worked to establish effective mechanisms for cooperation on cybersecurity with numerous countries. Beyond its role within the Shanghai Cooperation Organization, China has participated in specialized working groups on information and communication technologies (ICTs). These include the UK-China Internet Roundtable, U.S.-China Internet exchanges and forums, the China-France Joint ICT Committee, trilateral ministerial dialogues among China, Japan, and South Korea, and the China-Pakistan ICT Industrial Cooperation Working Group. China's successful experiences with these mechanisms should contribute to broader

international efforts for information security cooperation under the framework of the United Nations. These initiatives reflect China's commitment to advancing international collaboration in cybersecurity (Nagorski, 2010, p. 3).

Conclusion

Given the increasing importance of cyberspace and its critical role in ensuring the national security of countries, particularly China, as one of the leading global actors, this study demonstrates in response to the main research question that cyberspace is not only a new arena for competition and security threats but also a crucial platform for China's security and social policymaking. Theoretical studies on "securitization" show that cybersecurity extends beyond the military dimension, encompassing economic, political, and social spheres, and understanding this reality is essential for policymakers.

According to securitization theory, security is not merely a military or physical issue; it can encompass various political, economic, cultural, and social domains. More importantly, security is a constructed concept produced and reproduced through social and political processes. In this theory, states and political actors transform various issues into urgent and vital security matters through "securitization," which requires immediate and special action. As an emerging and complex domain, cyberspace represents a new challenge in national security. By securitizing cyberspace, China has transformed it from a purely technological sphere into a vital security issue that demands control, oversight, and specialized policymaking.

With a defensive-offensive approach and extensive investment in advanced security technologies, China has addressed cyber threats in line with global technological developments and established its position as a global cyber power. By adopting strict strategies for monitoring and controlling cyberspace, including establishing advanced systems such as the Social Credit System, Skynet, and the Golden Shield Project, the Chinese government has successfully maintained political and social stability and prevented potential threats to the regime.

Ultimately, this study emphasizes that information control and precise cyber regulatory policies are key to China's national security strategy. Through these tools, the Chinese government has been able to effectively counter emerging cyber threats and ensure its security in the digital age. China's approach is a model for how security policies can adapt to a rapidly transformed technological and communicative world, offering valuable lessons for other nations.

References

Alberts, D. S., & Papp, Daniel. (2010). Selections from Cyberspace: National Security Requirements in the Internet Age. Translated by Ali Aliabadi & Reza Nakhjavani. Tehran: Strategic Studies Research Center.

Amini, A. (2004). China's Information Warfare Doctrine. Psychological Operations Quarterly, No. 5.

Beach, D. (2012). Analyzing Foreign Policy, United Kingdom, Privilege Macmillan

Clark, I. (2007). Globalization and International Relations Theory. Translated by Faramarz Taghilou, Tehran: Office of Political and International Studies.

Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work, and social management for the twenty-first century. Journal of contemporary China, 26(103), 85-100

Feldstein, S. (2021). The Rise of Digital Repression: How Technology is Reshaping Power, Politics and Resistance. Oxford University Press, 212

Fritz, J. (2008). How China will use cyber warfare to leapfrog in military competitiveness, Culture Mandala: The Bulletin of the Center for East-West Cultural & Economic Studies, 8 (1)

Khalilipur Rokn Abadi, et al. (2012). Cyber Threats and Their Impact on National Security. Strategic Studies Quarterly, No. 56.

Mishra, V., & Arun Teja Polcumpally. (2021). Understanding Chinese media censorship: From Ming to Jinping. Observer Research Foundation. Retrieved from https://www.orfonline.org.

Mozaffarinia, M. (2023). Cyber Power: Nature, Dimensions, Capabilities, and Global Indicators. Research Center of the Islamic Consultative Assembly.

Nagorski, A. (2010). April Global Cyber Deterrence, Views from China, the U.S., Russia, India, and Norway.

Rezapour, M. M. (2019). Cyber Governance in China. National Center for Cyberspace Studies - Group for Science and Emerging Technologies, Report No. 19.

Strittmatter, K. (2020). We have been harmonized: Life in China's Surveillance State. HarperCollins 163-178

Zarif, M. J., et al. (2025). Security and Securitization in International Relations (Case Study: Securitization in the Islamic Republic of Iran). Geopolitics Quarterly, 21st Year, No. 1.