Journal of Sociology & Cultural Research Review (JSCRR)
Available Online: https://jscrr.edu.com.pk
Print ISSN: 3007-3103 Online ISSN: 3007-3111
Platform & Workflow by: Open Journal Systems

# SINO-RUSSIA CYBER ALLIANCE: AI-DRIVEN THREATS TO US NATIONAL SECURITY

**Shawal Saqib**
Department of Political Science and International Relations, University of Management and Technology, Lahore Pakistan
f2024112010@umt.edu.pk

## ABSTRACT

*The Sino-Russian cyber alliance represents a formidable challenge to U.S. national security, characterized by its focus on leveraging artificial intelligence (AI) to enhance cyber warfare capabilities. This partnership exploits vulnerabilities in democratic institutions, targets critical infrastructure, and undermines global stability. By analysing the evolution of this alliance and its AI-driven strategies, this research examines the historical and contemporary dimensions that underpin their objectives to counter U.S. dominance and promote a multipolar world order. The study explores how AI technology has enabled China and Russia to conduct advanced cyber operations, including precision strikes, automated reconnaissance, and large-scale disinformation campaigns. Their coordinated policies, such as China's "Cyber Sovereignty" doctrine and Russia's "Sovereign Internet" law, have fortified their domestic digital control while fostering deeper collaboration in intelligence sharing and offensive strategies. The integration of AI into cyber operations has also elevated threats to critical infrastructure, such as energy grids and healthcare systems, amplifying the economic and security risks to the U.S. This paper highlights key elements of the Sino-Russian alliance, including their shared resources, joint operations, and policy alignment, which collectively shape global cyber norms in their favour. It concludes with actionable recommendations for U.S. policymakers to strengthen national cybersecurity defences, mitigate risks to critical infrastructure, and foster international alliances to counterbalance the growing influence of this cyber partnership.*

***Keywords:*** *Cyber Warfare, Artificial Intelligence, Sino-Russian Alliance, U.S. National Security, Critical Infrastructure, Disinformation Campaigns*

## INTRODUCTION

The strengthening partnership between Sino-Russia has reshaped the global cybersecurity landscape. Their collaboration in cyberspace increased over time accompanied by their shared geopolitical ectives and opposition to the US. This collaboration and alliance also resulted in the development and deployment of AI-powered cyber tools, that allow both nations to conduct sophisticated operations against their adversaries, most notably the US. Both nations seek to counterbalance U.S. influence globally and promote a multipolar world order. (Richard Weitz, 2024)

For the sake of this study, we can define "cyber warfare" as, state or non-state actors operating within the sovereignty of a nation-state, that engaged in cyber-enabled activities at or below the level of armed conflict. Cyber operations are inherently revolutionized by artificial intelligence, which empowers attackers to improve their invasion measures, enhance efficiency, and adapt to countermeasures in a given time. AI-driven systems have unilaterally given China and Russia the ability to execute precision strikes, automate reconnaissance, and conduct psychological operations at new scales.

In addition, cyberspace has emerged as a key battleground for the Sino-Russian alliance and their aim to challenge the rules-based international order that the US has established and dominated. AI is seen as a key factor in developing advanced weaponry and military strategies (George S. Takach, 2024). The collaboration between China and Russia is shaping the global cyber norms in their favor, beyond the parameters of technology, policy alignment, and coordinated strategies. With the advancement of AI technology, the threat of this collaboration only intensifies, requiring the immediate attention of US policymakers and stakeholders.

China and Russia have strategically aligned their cyber strategies and policies to counter Western influence and consolidate their hegemony. China's "Cyber Sovereignty" doctrine emphasizes state sovereignty over the internet data and infrastructure and advocates national firewalls and digital borders. Russia has implemented a "Sovereignty Internet" law, with similar restrictions to China that grants the state more sovereignty over online content and communication networks. These policies enhance domestic surveillance capabilities while reducing the Western digital influence by a controlled cyber environment.

Furthermore, both nations have strengthened their legislative frameworks to support cyber operations. China's 2023 amendments to its Data Security Law imposed strict rules on data localization, preventing foreign entities from threatening and accessing classified information. The Russian Federal Security Service (FSB) has expanded its cyber law scope, allowing proactive cyber countermeasures against external threats. These policy improvements allow increased and deeper cooperation in cyber intelligence sharing, AI analysis, and coordination of disinformation campaigns, posing a direct challenge to US cyber interests.

## LITERATURE REVIEW

The Sino-Russian cyber alliance, characterized by its integration of artificial intelligence (AI), has garnered significant attention in the fields of cybersecurity and international relations. Existing literature underscores the growing sophistication of cyber threats posed by this partnership, particularly its implications for U.S. national security and global stability.

Barry Buzan's security framework (*People, States, and Fear*, 1991) emphasizes the multifaceted nature of security threats, including technological dimensions. Applying Buzan's lens, researchers such as Lewis (2018) and Rid (2020) have explored how China and Russia exploit cyberspace to achieve strategic dominance. Their shared ambition for a multipolar world order challenges Western technological supremacy through coordinated cyber operations and AI innovations.

China's "Cyber Sovereignty" doctrine, analysed by Creemers (2016), highlights its intent to assert control over domestic and global internet infrastructure. Complementing this, Russia's "Sovereign Internet" law, as explored by Soldatov and Borogan (2019), aims to shield its cyberspace while enabling offensive capabilities. Together, these policies reflect a convergence of interests in countering U.S. influence.

AI's role in enhancing cyber warfare capabilities is a recurring theme in contemporary studies. Kissinger et al. (2021) argue that AI-driven automation in cyber operations has escalated the scale and precision of attacks, with implications for critical infrastructure and information warfare. Disinformation campaigns, as examined by Chertoff (2019), have further

undermined public trust in democratic institutions, with China and Russia leveraging AI to amplify these effects.

Despite extensive studies on Sino-Russian cyber activities, gaps remain in understanding the operational dynamics of their alliance. Contributions by Giles (2016) and Segal (2020) focus on the strategic objectives of the partnership but fall short of addressing the technological interoperability enabled by AI. Additionally, limited research exists on the global ramifications of this alliance, particularly its influence on international cyber norms.

This literature review establishes the foundation for investigating how the Sino-Russian cyber alliance, powered by AI, disrupts U.S. security and critical infrastructure. Building on existing frameworks, the study contributes to bridging gaps by analysing the operational synergies between China and Russia and proposing countermeasures for U.S. policymakers to mitigate emerging threats.

## RESEARCH QUESTIONS

1. How has the Sino-Russia cyber alliance evolved, and what are its strategic objectives?
2. What roles does AI play in enhancing the cyber capabilities of China and Russia?

## THEORETICAL FRAMEWORK

This study analyzes the Sino-Russia cyber alliance by applying a realist framework. By emphasizing the power dynamics and national interest under Realism, it provides a lens to understand why China and Russia collaborate in cyberspace to challenge US dominance. Russia and China have evolved their cyber warfare capabilities to be executed almost exclusively in the digital gray zone of international law-the area where traditional rules and principles do not apply clearly. (M.G. Mclaughlin and W.J. Holstein, 2023). This study also incorporates cybersecurity theories focusing on threat modeling, risk assessment, and the role of technology in shaping offensive and defensive strategies.

## METHODOLOGY

This study employs a qualitative research design, relying exclusively on secondary data to analyze the implications of the Sino-Russian cyber alliance, augmented by artificial intelligence (AI), on U.S. national security and global stability. The focus is on

understanding patterns, strategies, and the broader geopolitical context through an in-depth examination of secondary sources.

Data Collection: Document Analysis: The study uses publicly available reports from credible organizations such as the United Nations, cybersecurity think tanks, and national intelligence agencies. Key sources include policy papers, cybersecurity white papers, and international relations journals.

Media and Academic Publications: News articles from established outlets, books, and peer-reviewed journal articles provide additional insights into the activities and strategies of the Sino-Russian alliance.

Historical Data: Historical incidents of cyberattacks and AI integration in cybersecurity operations are examined to draw patterns and predict future trends.

Analytical Framework: Barry Buzan's theoretical lens (People, States, and Fear) guides the analysis, focusing on the interplay between national security and transnational cyber threats. A narrative analysis approach is employed to identify recurring themes, such as AI-driven cyber warfare, misinformation campaigns, and the evolving geopolitical landscape.

Data Analysis: Data is coded thematically to highlight key trends, such as the methods used in cyberattacks, their political and economic motivations, and their consequences for U.S. security. Cross-referencing various sources ensures the reliability of insights.

Limitations:

- Dependence on Secondary Data: The study is constrained by the availability and reliability of secondary data, which may be outdated, biased, or incomplete. Access to classified or restricted information could provide a more comprehensive understanding of the topic, but such data remains inaccessible.
- Potential Bias: Secondary sources, particularly media reports and government documents, may reflect the agendas or priorities of their publishers. This introduces the risk of skewed interpretations. Efforts are made to mitigate this by consulting multiple sources and cross-verifying information.
- Lack of Real-Time Insights: The reliance on historical and published data limits the ability to analyze rapidly evolving technologies and strategies in AI-driven cyber warfare.

- Subjectivity in Interpretation: Narrative analysis, while useful for exploring themes, is inherently subjective and may reflect the researcher's perspective. Triangulating findings from diverse sources helps reduce this bias.

## RESULTS AND DISCUSSION

The history of China and Russia's partnership in cyberspace began in the early 2000s. China has framed primarily in terms of the right to non-interference in a state's internal affairs. On the other hand, Russia's policy to discourse on 'information security' has a longer lineage, but is essentially aligned with many of the aforesaid goals of China. First articulated in the 2000 Doctrine on Information Security, this concept is presented as a 'triad' of state, society, and individual interests (Arun Sukumar and Arindrajit Basu, 2024). Over time, this partnership gained significant momentum with the 2015 agreement on information security cooperation. This formalized their cyber collaboration, focusing on countering Western influence and sharing resources to strengthen their cyber capabilities (US Department of Homeland Security, 2024).

The strategic objectives of the Sino-Russia partnership revolve around undermining US influence by targeting critical infrastructure, financial systems, and political processes to weaken US global dominance. Besides, it promotes authoritarian values by countering democratic ideals through coordinated propaganda and disinformation campaigns. It also strengthens domestic regimes by using cyber tools to suppress dissent and control information within their borders (Reuters, 2013). China and Russia's pursuit of cyber sovereignty and information security is largely animated by the survival of its political institutions and the quest for social stability (Barrinha and Turner 2024; Flonk, Jachtenfuchs, and Obendiek 2020; Gao; Jiang 2010; Nocetti 2015).

These are covert cyber-attacks that involve an unauthorized intruder that gains access to a network to access sensitive data and remains undetected for a prolonged time. In China, groups like Volt Typhoon, Salt Typhoon, Wicked Panda (APT 41), Goblin Panda (APT 27), and Hafnium use machine learning and malicious files to infiltrate networks and for reconnaissance. These groups use AI algorithms to automate data collection and identify high-value targets that make them more efficient in their operations. As for Russia, Cozy Bear (APT 29), and Fancy Bear (APT 28) establish AI to create polymorphic malware and

optimize attack vectors. Through AI, the development of such malware increased which adapts to evade detection by making traditional cybersecurity measures outdated (Carnegie Endowment for International Peace, 2024).

Using deepfake technology and social media bots through AI enables large-scale campaigns to undermine trust in democratic processes and polarize public opinion. For example, during the 2024 US election cycle, AI-generated content spread false narratives, fueling societal divisions (Council on Foreign Relations, 2025). Manipulating public discourse through misleading content and creating fake personas are also involved in disinformation campaigns. Several AI tools analyze user behavior to reshape propaganda for maximum impact to target specific demographics by leveraging psychographic profiling.

Public institutions and critical infrastructure are rapidly becoming top targets for cybercrime around the globe. Sino-Russia uses these ransomware attacks through AI as leverage for disrupting energy grids and transportation systems. For instance, a 2023 attack on a US-based energy provider used AI-driven ransomware to encrypt critical systems and demand payments in cryptocurrency, crippling operations for days (MIT Technology Review, 2023). Furthermore, in 2024, the US's biggest healthcare payment system operated by Change Healthcare which handles some 14 billion transactions a year took a hit from a ransomware attack carried out by the Blackcat/ALPHV ransomware group (Anapaya, 2024).

AI also enhances vulnerability identification and the ability to explore critical infrastructure. This has enabled minimizing the resources required, more precise attacks, and an increase in the success rate of cyber operations.

In the growing economic, military, diplomatic, and technological relations, China and Russia share AI development and research resources for creating advanced cyber tools through expertise. Both nations stay ahead of Western technology advancements by exchanging joint AI training programs, talent sharing in high-tech industries, and knowledge about AI-enhanced logistics, trade, and transportation systems along with expertise in big data and quantum computing.

Apart from that they shared investment and expertise in missile technology, electronic warfare, and surveillance. China and Russia have joint AI-driven military projects as well that include

autonomous weapons and cyber warfare. They have joint development of smart cities and digital infrastructure and the expertise that enables them to use AI-driven management for oil, gas, and energy projects.

By leveraging their respective strength, coordinated attacks have become more frequent with both China and Russia. They exchange intelligence on cyber threats, vulnerabilities, and adversary tactics. Both nations developed AI-powered cybersecurity frameworks and collaboration in protecting critical infrastructure from cyberattacks by joining research on offensive and defensive cyber warfare techniques. While China excels in data collection and technology innovation, Russia specializes in psychological operations and propaganda.

Both nations have unified stances and aligned policies on international AI governance, advocating for state sovereignty in internet regulation, and, cyberspace governance. These alignments strengthen their ability to establish alternative AI standards to counter international norms that favor an open and free internet, challenging US-led initiatives and regulations. Beijing and Moscow's cooperation is driven by their desire to curb American power and challenge U.S. hegemony (Clara Fong and Lindsay Maizland, 2024).

Implications for US National Security

- Threats to Democratic Institutions: The legitimacy of elections and governance is eroding through AI-driven disinformation campaigns that undermine public interest in the democratic process. The risk of deepfakes, AI-enabled misinformation campaigns, and automated hacking tools is increasing (Clark, R. A., and Knake, R. K., 2024).
- Economic Impact: Financial systems and critical infrastructure are getting targeted by cyberattacks that have devastating economic consequences. The cost of ransomware attacks and data breaches has risen exponentially, with the average cost of a breach reaching $10 million by 2025 (Brookings Institution, 2024).
- Erosion of Technological Leadership: The US leadership is threatened by the Sino-Russia alliance in AI and cybersecurity. AI can both bolster and undermine cybersecurity efforts, presenting new challenges such as sophisticated cyberattacks and automated hacking tools

(Lin, H., 2023). China and Russia are narrowing the gap by accelerating their technological development, challenging US dominance in these critical areas. Disparities in AI capabilities can influence the balance of power in cyberspace, potentially leading to increased vulnerability for less technologically advanced countries (Bradshaw, S., and Howard, P. N., 2023).

## RECOMMENDATIONS

- Western nations need to respond, including enhancing their own technological innovation and fostering alliances to counterbalance Sino-Russian advancements (Cheung, T. M., and Ho, J., 2024). These nations have to invest in AI for cybersecurity and to develop AI-driven tools to detect and respond to cyber threats in real-time.
- The collaboration between government agencies and private companies should enhance their Public-Private partnership to share intelligence and resources.
- To prevent misuse and threats, robust regulations and standards for AI development and cybersecurity should be established and implemented. The challenges in AI deployment in cybersecurity, including ethical considerations, and potential biases in AI models, need to be learned and understood to adapt to the evolving threats (Zhang, W., and Liu, Y., 2024).

### International Collaboration

- Western states should strengthen and forge their ties with allies to create a unified front against cyber threats.
- By advocating and promoting their norms and standards for international agreements on responsible and harmless behavior in cyberspace.
- Western nations along with other developed nations can assist developing nations by supporting their capacity building and improving their cybersecurity capabilities to prevent exploitation by adversaries.

### Public Awareness and Education

- Launching initiatives to educate and combat disinformation and make the public aware of identifying and countering false narratives.

- Encouraging critical thinking, promoting digital literacy, and responsible online behavior to reduce their inclination to get manipulated.

## CONCLUSION

Geopolitical constraints provide Russia and China with a plethora of reasons to band together. Their distrust of Western hegemony, authoritarian governments, and similar political ambitions have nurtured relations between Moscow and Beijing for the last political generation (Fraser, C., 2024). The Sino-Russia cyber alliance and strategic application to cyber operations through AI advancements are considered an unprecedented challenge and potential threat to US national security. Both sides have been framing their perceived rivals' AI capabilities as threats to national security and strategic stability (Nadibaidze, A., 2024). By leveraging AI, China, and Russia have enhanced their ability to disrupt critical infrastructure, conduct sophisticated cyberattacks, and undermine democratic institutions. To address these threats and challenges, an approach that includes international collaboration, public engagement, and most importantly advanced technological innovations is required. To protect and safeguard US national security and interest while maintaining hegemony in the digital age, the state needs to take essential proactive measures by investing in AI cybersecurity tools, promoting global norms, and, strengthening alliances for responsible behavior in cyberspace.

## REFERENCE

Barrinha, A., & Turner, R. (2024). Strategic narratives and the multilateral governance of cyberspace: The cases of European Union, Russia, and India. *Contemporary Security Policy, 45*(1), 72–109. https://doi.org/10.1080/13523260.2023.2266906

Bradshaw, S., & Howard, P. N. (2023). Challenging the digital divide: AI in global cyber conflicts. *International Journal of Cyber Studies, 15*(3), 201–220.

Brookings Institution. (2024). Strategic rivalries in the cyber domain: Sino-Russia collaboration. Retrieved from https://www.brookings.edu

Candan, B. (2024). Top 5 critical infrastructure cyberattacks. Retrieved from https://www.anapaya.net/blog/top-5-critical-infrastructure-cyberattacks

Carnegie Endowment for International Peace. (2024). AI and cybersecurity: Challenges and opportunities. Retrieved from https://www.carnegieendowment.org
Cheung, T. M., & Ho, J. (2024). *Sino-Russian technology partnerships: Implications for the West*. Routledge.
Clarke, R. A., & Knake, R. K. (2024). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Random House.
Council on Foreign Relations. (2025). AI-driven disinformation: Impacts on US elections. Retrieved from https://www.cfr.org
Flonk, D., Jachtenfuchs, M., & Obendiek, A. S. (2020). Authority conflicts in internet governance: Liberals vs. sovereigntists. *Global Constitutionalism, 2*, 364–386.
Fong, C., & Maizland, L. (2024). China and Russia: Exploring ties between two authoritarian powers. Retrieved from https://www.cfr.org/backgrounder/china-russia-relationship-xi-putin-taiwan-ukraine
Fraser, C. (2024). Russia and China: The true nature of their cooperation. Retrieved from https://rusi.org/explore-our-research/publications/commentary/russia-and-china-true-nature-their-cooperation
Gao, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the Western model. *International Spectator, 57*(3), 15–30.
Jiang, M. (2010). Authoritarian informationalism: China's approach to internet sovereignty. *SAIS Review of International Affairs, 30*(2), 71–89.
Lin, H. (2023). *Cybersecurity futures: Emerging threats and solutions*. Oxford University Press.
MIT Technology Review. (2023). The rise of AI in cyber warfare. Retrieved from https://www.technologyreview.com
Nadibaidze, A. (2024). Russia's drive for AI: Do deeds match the words? *The Washington Quarterly, 47*(4), 137–154. https://doi.org/10.1080/0163660X.2024.2435162
Nadibaidze, A. (2024). Russia's drive for AI: Do deeds match the words? *The Washington Quarterly, 47*(4), 137–154. https://doi.org/10.1080/0163660X.2024.2435162
Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs, 91*(1), 111–130.

Reuters. (2023). Sino-Russia cyber cooperation intensifies with AI integration. Retrieved from https://www.reuters.com

Sukumar, A., & Basu, A. (2024). Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order. *Journal of Cyber Policy, 1*(1), 1–32. https://doi.org/10.1080/23738871.2024.2436591

Takach, S. G. (2024). *Cold War 2.0: Artificial intelligence in the new battle between China, Russia, and America*.

US Department of Homeland Security. (2024). *Global cyber threat report*. Washington, DC: DHS Publications.

Weitz, R. (2024). *The new China-Russia alignment: Critical challenges to U.S. security.*

Zhang, W., & Liu, Y. (2024). Artificial intelligence in modern cybersecurity frameworks. *Journal of Strategic Security, 12*(4), 145–162.