SUPREMO AMICUS

VOLUME 39 | October, 2025 ISSN 2456-9704

CYBER SECURITY AS A TOOL OF STATECRAFT : A COMPARATIVE STUDY OF THE US, CHINA AND RUSSIA

By *Dr Rajesh Kumar Singh*
Assistant Professor at Babu Jagjivan Ram Institute of Law, Bundelkhand University

Abstract

In the digital age, cybersecurity has emerged as a pivotal element of national power, shaping not only defense strategies but also foreign policy, economic competition, and ideological influence. This paper presents a comparative analysis of how the United States, China, and Russia weaponize cybersecurity within their broader strategic cultures. The United States employs a doctrine of deterrence and norm entrepreneurship, emphasizing persistent engagement and global governance leadership. China integrates cybersecurity into its model of techno-nationalism, prioritizing cyber sovereignty, regime control, and the global export of surveillance infrastructure. Russia, by contrast, uses cyberspace asymmetrically to wage covert operations, disinformation campaigns, and disruptive influence across geopolitical fault lines. Through doctrinal review, institutional analysis, and geopolitical context, the study illustrates how cybersecurity functions as both a tactical instrument and a strategic language of modern statecraft. The findings reveal a deepening cyber power divide and underscore the risks of normative fragmentation in the governance of cyberspace.

Keywords: Cybersecurity, Statecraft, Cyber Sovereignty, Cyber Warfare, United States, China · Russia, Digital Geopolitics, Information Warfare, Cyber Strategy, Techno-Nationalism, Norm Entrepreneurship, Disinformation, Strategic Competition

Introduction

In the 21st century, cybersecurity has evolved from a technical concern into a central instrument of modern statecraft. Once seen as the domain of IT departments, it now sits firmly at the heart of national security strategies, foreign policy doctrines, and even economic competition among major powers. As the world becomes increasingly interconnected through digital infrastructure, states are leveraging cyber tools not just for defense, but to project power, influence rivals, and shape global norms.

Among the leading cyber powers, the United States, China, and Russia stand out for their sophisticated, yet contrasting approaches to using cybersecurity as a strategic instrument. Each country frames cyberspace in line with its political ideology and strategic objectives: the U.S. promotes a free and open internet, China asserts a model of cyber sovereignty and domestic control, and Russia weaponizes cyber tools for asymmetric warfare and political disruption.

As Lindsay (2025) puts it, cyber operations have transitioned from isolated acts of hacking to a permanent feature of state behavior, blurring the lines between peace and conflict. Cyber tools are not just used for surveillance or defense—they are actively integrated into foreign policy, deterrence strategies, and economic statecraft.

"Stuxnet and SolarWinds didn't just damage systems—they revealed a new form of secret statecraft at work in cyberspace."

— *Lindsay, J. (2025)*

This transformation is especially clear in China’s digital authoritarianism, where cybersecurity is used to enforce internal control and export surveillance technologies through its Digital Silk Road initiative. As Wong (2021) observes, China’s cybersecurity laws serve a dual purpose: protecting regime stability at home and enhancing technological dominance abroad.

“Cybersecurity in China is more than a defensive shield—it’s a platform for political control and digital geopolitics.”
— Wong, P.N. (2021)

Meanwhile, Russia approaches cyberspace as a tool of non-linear warfare, favoring ambiguity, proxy actors, and psychological operations. As Grzegorzewski and Marsh (2024) explain, Russia’s strategy focuses less on deterrence and more on disruption, confusion, and undermining adversary cohesion—a reflection of its broader geopolitical posture.

“Russia’s cyber toolkit reflects its deep investment in information operations, combining cyberattacks with narrative warfare.”
— Grzegorzewski, M. & Marsh, C. (2024)

This paper provides a comparative analysis of how the U.S., China, and Russia weaponize cybersecurity—not merely as a protective measure, but as a flexible instrument of power projection, political influence, and norm-setting. Through this lens, cybersecurity emerges not just as a technical necessity, but as a geopolitical language through which states articulate their ambitions, ideologies, and anxieties in the digital age.

The United States: Cyber Superiority and Norm Entrepreneurship

The United States has long been at the forefront of global cyber power, leveraging its technological dominance, robust private sector, and global alliances to establish itself as a leader in both cyber capability and cyber governance. Its approach to cybersecurity as statecraft is built around two primary pillars: maintaining superiority in offensive and defensive capabilities, and shaping global norms and regulations in cyberspace—a dual strategy often described as “cyber superiority and norm entrepreneurship”.

Strategic Vision and Doctrinal Shift

The U.S. Department of Defense officially recognized cyberspace as a warfighting domain in 2011. This acknowledgment was formalized in the 2018 DoD Cyber Strategy, which introduced the concept of "persistent engagement" and the need to "defend forward." This strategy advocates proactive cyber operations—not just defending American networks, but disrupting malicious cyber activity at its source, often in foreign cyberspace before it reaches U.S. targets.

As Lindsay (2025) notes, this shift represents a fundamental evolution in U.S. cyber doctrine, from passive deterrence to active cyber competition. Cyber operations like Stuxnet (which targeted Iran’s nuclear centrifuges) and the exposure of Russian interference in the 2016 U.S. elections illustrate how the U.S. has developed and employed cyber tools for strategic objectives.

“Persistent engagement isn’t just about resilience—it’s about reshaping the adversary’s decision calculus by imposing real-time costs in cyberspace.”

— *Lindsay, J. (2025)*

Institutional Framework and Operational Capacity

The operational backbone of U.S. cyber strategy is the United States Cyber Command (USCYBERCOM), which works closely with the National Security Agency (NSA) under a dual-hat leadership. This alignment allows the U.S. to integrate signals intelligence (SIGINT) with military cyber operations, offering unmatched visibility into foreign networks.

Complementing this military-cyber integration is the Cybersecurity and Infrastructure Security Agency (CISA), formed in 2018 to protect civilian infrastructure, especially in light of increased ransomware threats and foreign interference in domestic elections.

According to Grzegorzewski & Marsh (2024), U.S. cyber power lies not just in government capabilities but in its collaboration with the private sector, which controls most of the country's critical infrastructure and advanced technologies.

"In the U.S., the fusion of military doctrine with Silicon Valley innovation produces a hybrid cyber ecosystem where deterrence, defense, and diplomacy are co-produced."

— *Grzegorzewski, M. & Marsh, C. (2024)*

Cyber Diplomacy and Norm Setting

Beyond its military operations, the U.S. plays a leading role in international cyber governance. It champions an "open, interoperable, secure, and reliable internet" and has used forums such as the United Nations Group of Governmental Experts (UNGGE) and the Paris Call for Trust and Security in Cyberspace to advocate norms against state-sponsored cybercrime, IP theft, and targeting of civilian infrastructure.

This posture stands in contrast to authoritarian models promoted by China and Russia, who seek to define "cyber sovereignty" and limit the role of multistakeholder internet governance. In this ideological divide, the U.S. acts as a norm entrepreneur, promoting a liberal vision of cyberspace rooted in transparency, rule of law, and international cooperation.

As Aljameele (2025) argues, the U.S. combines its technical superiority with regulatory leadership, influencing the global digital order through both coercive power (military and sanctions) and normative influence (standards and treaties).

"The U.S. exports not only its technologies, but also its cybersecurity values and regulatory blueprints, shaping a digital ecosystem that aligns with its geopolitical interests."

— *Aljameele, M. (2025)*

China: Cyber Sovereignty and Techno-Nationalism

China's approach to cybersecurity is fundamentally shaped by its authoritarian political system, its national developmental model, and its vision of digital sovereignty. Unlike the U.S., which promotes an open and interoperable cyberspace, China treats cyberspace as a sovereign domain—an extension of the state's territorial authority, subject to strict control and censorship. This principle, often described as "cyber sovereignty," is the core of China's cyber doctrine and reflects its broader political goals of regime stability, national rejuvenation, and technological self-reliance.

Doctrinal Foundations: Cyber as a Tool of Control and National Power

The Chinese Communist Party (CCP) sees cyberspace not just as a domain of competition but also as a strategic frontier for ensuring internal security, controlling information flows, and asserting geopolitical influence. According to Cai (2016), Chinese cybersecurity policy is explicitly linked to political control—particularly the CCP's need to monitor and suppress dissent, protect party legitimacy, and avoid external ideological influence.

"For China, cyberspace is not a commons but a territorialized, securitized domain, tightly integrated with the interests of the state and the party."

— *Cai, C. (2016)*

This perspective was codified in the 2017 National Cybersecurity Law, which mandates that all network operators store user data in China and submit to government inspection. The 2015 National Security Law and the 2015 Counterterrorism Law further solidified legal authority for broad surveillance and censorship powers, creating a legal infrastructure that links cybersecurity to state security.

Strategic Capabilities: Surveillance, Espionage, and Infrastructure Dominance

China's cyber capability is orchestrated through the People's Liberation Army Strategic Support Force (PLASSF), which merges cyber, electronic, and psychological warfare. It also operates through the Ministry of State Security (MSS), responsible for foreign intelligence and cyber espionage, often via proxy hacker groups such as APT10 and APT41.

Beyond military power, China has developed a vast domestic surveillance ecosystem, underpinned by facial recognition, biometric databases, and the Social Credit System—a technological framework of behavioral monitoring and control. These capabilities reflect the CCP's goal of integrating cybersecurity with broader ambitions of technological dominance and social management.

As Kolodii (2020) notes, "China's integration of cybersecurity with surveillance tech marks a unique model of authoritarian digital governance, increasingly exported to other regimes."

— *Kolodii, R. (2020).*

China's cyber espionage is also driven by industrial and technological goals, particularly the ambition to reduce reliance on foreign suppliers. As part of the "Made in China 2025" initiative and the 14th Five-Year Plan, China aims to become self-sufficient in key digital technologies, including semiconductors, AI, and cloud computing. Cyber intrusions targeting Western tech firms and universities have often been linked to this industrial agenda.

"Cyber operations are a pillar of China's techno-nationalism—used not only for defense but also to advance strategic economic priorities."

— *Wong, P.N. (2021).*

Digital Diplomacy and the Global Export of Cyber Sovereignty

China's cyber strategy is not confined within its borders. Through the Digital Silk Road—a component of the Belt and Road Initiative—China exports its digital infrastructure, cybersecurity models, and surveillance technologies to developing countries. This includes partnerships in Africa, Central Asia, Southeast Asia, and Latin America, where China offers low-cost 5G networks, smart city systems, and cybersecurity training, often bundled with loans and diplomatic engagement.

Prokopyshyn and Trushkina (2025) emphasize that China's digital diplomacy builds "infrastructure dependency and ideological alignment" with partner states, effectively spreading the principle of cyber sovereignty as a counterweight to Western norms.

— *Prokopyshyn, O., & Trushkina, N. (2025)*

At the United Nations and multilateral fora, China pushes for international recognition of cyber sovereignty—arguing that states should have the legal right to regulate the internet within their own borders. This stance has clashed with the Western vision of a decentralized, open internet, creating a global normative divide in cyberspace governance.

Criticism and International Concern

China's cybersecurity posture has attracted international criticism for its lack of transparency, cyber espionage campaigns, and authoritarian export model. Incidents such as the Office of Personnel Management (OPM) breach in the U.S. (2015), widely attributed to Chinese hackers, raised global alarms about the scale and ambition of China's state-sponsored cyber operations.

As Datta (2024) points out, the CCP's digital governance framework threatens liberal internet norms by showing that digital authoritarianism can be both scalable and exportable—posing a long-term challenge to democratic cyber governance.

"Where the U.S. builds partnerships through trust and interoperability, China builds them through dependency and surveillance incentives."

— *Datta, A. (2024)*

Russia: Disruption, Asymmetry, and Covert Statecraft

Russia's use of cybersecurity as a tool of statecraft is best characterized by asymmetry, ambiguity, and disruption. Unlike the United States, which builds cyber capability within a framework of deterrence and global norms, or China, which centers its strategy on cyber sovereignty and developmental nationalism, Russia weaponizes cyberspace as a grey zone battlefield, blending cyber operations with disinformation, political warfare, and covert influence campaigns. This approach is deeply rooted in Russia's broader non-linear warfare doctrine, often referred to as the Gerasimov Doctrine, which treats information space and cyberspace as domains for continuous, low-intensity confrontation below the threshold of open conflict.

As Grzegorzewski and Marsh (2024) argue, Russia's cyber strategy is not primarily about protecting infrastructure or promoting sovereignty—it is about shaping adversary behavior and undermining political cohesion through persistent digital disruption.

"Russia's cyber doctrine thrives on ambiguity, leveraging digital tools to erode the integrity of adversary institutions while maintaining plausible deniability."
— *Grzegorzewski, M., & Marsh, C. (2024).*

Strategic Doctrine: The Logic of Asymmetric Disruption

Post-Soviet Russia has prioritized the development of non-kinetic warfare capabilities, especially in cyberspace. Rather than compete symmetrically with Western technological and military superiority, Russia has adopted low-cost, high-impact methods of interference—targeting elections, critical infrastructure, media ecosystems, and political discourse in rival states. This reflects a long-standing KGB-era tradition of "active measures" (активные мероприятия), now digitally reimagined.

Russia's 2020 Information Security Doctrine formally integrates cyber operations into its national defense posture. It emphasizes defending Russia's "informational sovereignty", resisting "Western information aggression," and justifies preemptive cyber actions to protect national interests. These principles were demonstrated in events like:

The 2007 cyberattacks on Estonia, often regarded as the world's first major state-level cyber offensive.

The 2015 and 2016 attacks on Ukraine's power grid, which revealed Russia's ability to manipulate physical infrastructure remotely.

The 2016 U.S. election interference, where social media manipulation and data breaches were used to influence public opinion and trust.

As Lindsay (2025) notes, Russia's cyber operations are an extension of secret statecraft—tools designed to achieve political objectives without direct attribution or conventional military engagement.

"For Moscow, cyber operations aren't just tactical—they are strategic acts of political warfare executed in the shadows."
— *Lindsay, J. (2025).*

Operational Actors: State-Backed and Proxy Networks

Russia's cyber ecosystem is composed of both state institutions and quasi-autonomous hacker groups, which often serve as deniable assets. Key state actors include:

The Main Directorate of the General Staff (GRU) – particularly Unit 26165 and Unit 74455 (linked to APT28 or "Fancy Bear")

The Federal Security Service (FSB) – involved in surveillance and domestic cyber repression.

The Foreign Intelligence Service (SVR) – associated with APT29 or "Cozy Bear," implicated in espionage activities like the SolarWinds hack.

These agencies often operate through third-party groups or cybercriminals, giving Russia plausible deniability while conducting offensive operations. According to Datta (2024), this blurring of state and non-state lines is a hallmark of Russian cyber statecraft.

"Russia cultivates a strategic ambiguity by weaponizing a hacker ecosystem that is loosely state-affiliated but operationally deniable."

— *Datta, A. (2024).*

Russia also integrates cyber capabilities into military campaigns, most recently in Ukraine. The 2022 invasion was preceded by a wave of cyberattacks on Ukrainian government sites, demonstrating the integration of cyber operations with kinetic warfare.

Ideological Framing: Information Sovereignty and Defensive Narratives

Publicly, Russia frames its cyber activities as defensive, aimed at countering NATO expansion, Western digital colonialism, and information attacks on Russian values. This narrative is institutionalized through initiatives such as the "Sovereign Internet Law" (2019), which allows the state to isolate Russian cyberspace from the global internet in times of crisis.

As Kolodii (2020) explains, Russia's discourse around information security is not only about data protection but about preserving cultural and political control, often using cybersecurity laws to crack down on dissent and civil society.

"Russia conflates cybersecurity with state security, enabling the use of digital tools for domestic repression under the guise of resilience."

— *Kolodii, R. (2020).*

This ideological framing justifies actions that would otherwise be deemed cyber aggression under international law, and it helps normalize authoritarian digital governance, particularly among countries aligned with Russia geopolitically.

Global Implications: Norm Subversion and Influence Projection

Russia's approach to cyberspace challenges liberal international cyber norms by rejecting rules-based conduct and promoting state-centric digital sovereignty. It actively resists Western efforts at norm-building (such as the Paris Call or the UN Group of Governmental Experts) and instead supports initiatives that validate state control over internet infrastructure.

Moreover, Russia engages in strategic partnerships with authoritarian regimes like Iran and Belarus to share cyber expertise and jointly push for a new "digital multipolarity" that limits Western influence over global internet governance.

As Prokopyshyn and Trushkina (2025) emphasize, Russian cyber strategy represents a larger shift toward covert statecraft and digital coercion, enabled by its ability to operate in the margins of attribution and accountability.

"Russia's cyber statecraft is less about building influence than about eroding the legitimacy of others—a politics of sabotage rather than persuasion."
— *Prokopyshyn, O., & Trushkina, N. (2025).*

Comparative Analysis

To understand the divergent approaches to cybersecurity as a tool of statecraft by the United States, China, and Russia, a comparative matrix allows us to synthesize key elements of each country's doctrinal stance, strategic objectives, operational actors, and normative behavior. Despite being cyber powers, their policies are grounded in distinct political systems, threat perceptions, and international ambitions.

• **Dimension**	• **United States**	• **China**	• **Russia**
• **Cyber Doctrine**	• *Persistent engagement, defend forward,* deterrence-based	• *Cyber sovereignty, regime stability,* information control	• *Non-linear warfare, active measures,* strategic ambiguity
• **Strategic Objective**	• Maintain global cyber superiority, promote liberal norms	• Enhance internal control, assert digital sovereignty, achieve tech independence	• Undermine adversaries, protect regime, disrupt global order
• **Key Government Actors**	• USCYBERCOM, NSA, DHS, CISA	• PLASSF, Ministry of State Security, Cyberspace Administration of China	• GRU (APT28), SVR (APT29), FSB, "patriotic hackers"
• **Legal Framework**	• DoD Cyber Strategy (2018), National Cyber Strategy (2023), CISA Act	• National Cybersecurity Law (2017), National Security Law (2014)	• Information Security Doctrine (2020), Sovereign Internet Law (2019)
• **Operational Style**	• Targeted counter-operations, proactive defense, partnerships	• Integrated surveillance, state-ordered espionage, firewall systems	• Disruption, disinformation, proxy hacking, plausible deniability
• **International Behavior**	• Norm entrepreneurship, alliance building	• Export of digital infrastructure via Digital Silk Road,	• Norm resistance, strategic ambiguity,

	(NATO, QUAD, OECD)	push for cyber sovereignty norms	authoritarian tech export
• **Cyber Tools & Campaigns**	• Stuxnet, SolarWinds response, Microsoft Exchange hacks	• APT10, Great Firewall, biometric surveillance, Huawei tech	• NotPetya, DNC hacks, power grid attacks in Ukraine, troll farms
• **Digital Governance Model**	• Multi-stakeholder, rules-based internet	• State-centric, censored, surveillance-heavy	• Sovereign, state-controlled, anti-Western alignment
• **Strengths**	• Technological innovation, alliance ecosystem, offensive edge	• Centralized control, tech-industrial policy, global infrastructure export	• Low-cost disruption, narrative warfare, attribution resistance
• **Weaknesses**	• Bureaucratic fragmentation, private-sector dependency	• International trust deficit, sanctions vulnerability	• Innovation lag, diplomatic isolation, grey zone overuse

Findings from analysis

The United States sees cybersecurity as part of a broader strategic vision rooted in deterrence, technological leadership, and the promotion of global cyber norms. Its strength lies in offensive cyber operations and alliance cooperation but is challenged by coordination gaps and private-sector vulnerabilities.

China embeds cybersecurity within its authoritarian governance model and long-term techno-industrial ambitions. It views control of information space as crucial for regime survival and is actively exporting its model of cyber sovereignty, though facing growing resistance due to trust and transparency concerns.

Russia thrives on ambiguity and subversion, using cyber tools for asymmetric influence, especially in regions of strategic interest. While it excels in disinformation and disruption, its strategy is limited by international sanctions, technological dependence, and reputational damage.

Conclusion

In summary, while the United States, China, and Russia all recognize cyberspace as a critical domain of statecraft, their approaches reflect fundamentally different strategic cultures and political systems. The U.S. seeks to maintain cyber superiority through deterrence, innovation, and global norm-building; China emphasizes cyber sovereignty, internal control, and the projection of techno-nationalist influence; and Russia exploits cyberspace for asymmetric disruption, using covert operations to destabilize rivals and advance its geopolitical interests. These contrasting strategies not only shape global cybersecurity dynamics but also reflect a deeper contest over the future governance of the digital world.

References

- Aljameele, M. (2025). *Cybersecurity As Statecraft: International Regulatory Harmonization for a Secure Future*. Duke University. Retrieved from https://dukespace.lib.duke.edu/bitstreams/23714603-fb8f-4d11-875f-de0503c77293/download
- Cai, C. (2016). *Global Cybersecurity Environment: Perspectives of the US and China*. In *Securing Cyberspace*. Institute for Defence Studies and Analyses (IDSA). Retrieved from https://idsa.demosl-03.rvsolutions.in/publisher/system/files/book/book_securing-cyberspace_0.pdf#page=334
- Datta, A. (2024). *Trust, Interdependence, and Power in Cyber Statecraft*. SSRN. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4999418
- Grzegorzewski, M., & Marsh, C. (2024). *A Strategic Cyberspace Overview: Russia and China*. In D. Gioe & M. Smith (Eds.), *Great Power Cyber Competition* (Chap. 2). Taylor & Francis. Retrieved from https://www.taylorfrancis.com/chapters/edit/10.4324/9781003425304-2
- Kolodii, R. (2020). *Interstate Cooperation in Cyber Strategies of the United States and China Post-2010: A Comparative Study*. Charles University. Retrieved from https://dspace.cuni.cz/handle/20.500.11956/177210
- Lindsay, J. R. (2025). *Stuxnet Revisited: From Cyber Warfare to Secret Statecraft*. *Journal of Strategic Studies*. https://doi.org/10.1080/01402390.2025.2481447
- Prokopyshyn, O., & Trushkina, N. (2025). *The Geopolitics of Cybersecurity: A Comparative Analysis of National Strategies for Digital Sovereignty*. *Politics & Security*, 5(1). Retrieved from https://politics-security.net/index.php/ojsdata/article/view/282
- Wong, P. N. (2021). *Techno-Geopolitics: US–China Tech War and the Practice of Digital Statecraft*. Taylor & Francis. Retrieved from https://www.taylorfrancis.com/books/mono/10.4324/9781003047100

*****