JOURNAL OF POLITICAL STABILITY ARCHIVE

Online ISSN: 3006-5879 Print ISSN: 3006-5860
DOI: https://doi.org/10.63468/jpsa.3.3.08
Vol. 3 No. 3 (2025)
https://journalpsa.com.pk/index.php/JPSA/about

Recognized by: Higher Education Commission (HEC), Government of Pakistan

Securitizing Cyberspace: Use of Artificial Intelligence In Sino-American Relations and Its Impacts on India's National Security

Jannat Naseeb
MS. Security and Strategic Studies, University of Management and Technology

ABSTRACT

This research explores the securitization of cyberspace through the use of Artificial Intelligence (AI) in the context of Sino-American rivalry and examines its implications for the national security of India. The study addressed the rapid deployment of AI-powered technologies such as autonomous surveillance systems, cyber tools and psychological warfare techniques by USA and China, as a strategy for cyber confrontation. These measures not only reshape the bilateral relations but also exert pressure on regional powers like India to advance technologically in cyber domain. The main idea of the research is to analyze that how weaponization of AI in cyberspace is restructuring global power blocks structures and security postures while putting India at high risk of technological vulnerability, strategic ambiguity and digital exposure. This research incorporates qualitative methodology, where secondary sources like documents, literature and books were consulted to analyze the data. This research study also explores insights from the think tanks and other public-private policy formation institutes to assess the USA and China strategic cyber posture and India's response to it. Major findings are that while India is making regulatory reforms accordingly through international cooperation, it lacks a cohesive national AI-cybersecurity strategy and doctrine. It is important for India to strengthen its intuitions focusing on AI capabilities, increasing cyber diplomacy and institutionalizing rule-based approach to digital security and ensuring resilience in cyberspace.

Keywords: Securitization, Cyberspace, Artificail Intelligence, Diplomacy, Security, Surveillance, Weaponization

INTRODUCTION

Aerospace and high seas became important topics in earlier centuries cyberspace has evolved in past years and it has become a critical discussion in international relations. Cyberspace is even more important in international relations as there is no concept of border cyberspace is global and it cannot be limited to a

domestic or international sphere and it involves almost all human activities. The rise of artificial intelligence which is a subset of cyber space involving quantum computing machine learning and other new advancements does herald a new arm race in the world. With the advancement of Artificial Intelligence in cyberspace by major countries like USA and China the strategic competition continues to shape international security. The strategic competition in cyberspace between the United States and China, which lies at the intersection of conventional and unconventional aspects, also began in the last decade of the 20th century, when the two countries did not engage in confrontation and officially introduced cyberspace as a domain worthy of warfare. However, recognizing each other's and other countries' capabilities in cyberspace, they have begun to formalize cyberwarfare strategies and policy guidelines. As security situations around the world become increasingly volatile, the scale of escalation is harder to control, and complexities increase by the day, cyberwarfare specially use of AI has become the ideal weapon of choice with numerous advantages such as anonymity, lack of kinetic options, non-confrontations.

Today the cybersecurity landscape is characterized by dynamic threats, complex systems, and an evolving technological landscape. To effectively protect critical infrastructure and ensure national security, a multi-pronged approach is needed that transcends individual actors and relies on collaboration and collective efforts (Adegbite, Akinwolemiwa, Uwaoma, & Kaggwa, 2023).

The United States seeks to collaborate with its allies, partners, and stakeholders around the world to shape the design, development, governance, and use of cyberspace and digital technologies to promote economic prosperity and inclusion; strengthen security and combat cybercrime; promote and protect the exercise of human rights, democracy, and the rule of law; and address transnational challenges. The United States, working with its allies, seeks to: promote, build, and maintain an open, inclusive, secure, and resilient digital ecosystem; coordinate with international partners on rights-respecting approaches to digital governance and data; promote responsible government behavior in cyberspace and counter threats to cyberspace and critical infrastructure by building alliances and engaging partners; and strengthen and enhance the digital and cyberspace capabilities of international partners (US Department of State, 2025)

The U.S. cybersecurity strategy has evolved through three phases: "Comprehensive Defense, Asset Protection," "Joint Offense and Defense, Cyberterrorism," "Offensive Focus," and Network Deterrence. This strategy suggests that to effectively combat cybersecurity threats, a country must strengthen its own cybersecurity deterrence, be aware of its own strengths, and seize the initiative in the international space game (Huang).

Since the beginning of the 21st century, China has become a major player on the global stage, exerting significant influence over politics, the economy, and, most notably, cyberspace. According to the 2022 National Cyber power Index, China ranks second, behind the United States, and third, Russia. China's development in cyberspace is based on a clear strategy, including investments in advanced

infrastructure and technologies, as well as the implementation of innovative government policies. This development is attributable to international cooperation between its main partners, Russia and the BRICS countries. Beijing is working with these countries to promote cybersecurity and strengthen its global geopolitical influence. China's strategic investment in various global initiatives, such as the "Digital Silk Road" and the "Made in China 2025" plan, demonstrates its ambition to reshape the global financial and technological architecture. (Toma, 2024)

Chinese documents demonstrate that its experts take cyberwarfare very seriously. As the global economic system and military power increasingly rely on cyberspace, countries choose to seek asymmetric advantages and counterproductive means to achieve their military and political goals. To understand how the People's Republic of China dominates cyberspace, it is necessary to go beyond infrastructure, projects, and official statements (which are easier to quantify) and delve into China's cultural and philosophical foundations. (Knight, 2015).

Based on its own realities and learning from the experiences of other countries, China has created a unique model of cyberspace governance. On the path to building itself as a modern socialist country, China will always adhere to comprehensive and law-based governance of the country and cyberspace. It will promote the legal, orderly and healthy development of China's Internet, ensure the high-quality development of Digital China under the rule of law, and provide firm legal guarantees to strengthen China's cyberspace (The State Council Information Office of the People's Republic of China, 2023)

India is widely regarded as a rising power in the Global South and a staunch advocate of global institutional reform. Its cybersecurity policy should be understood as the result of integrated priorities that differ from those of other states addressing cybersecurity: domestically, it is about harnessing digital technologies to drive economic growth and social development; geopolitically, it is about reducing dependence on China and strengthening domestic counterbalancing capacity by improving cybersecurity, resilience, and developing offensive cybersecurity capabilities; and globally, it is about playing a constructive, even pioneering, role in multilateral normative debates on responsible behavior in cyberspace, emphasizing the importance of respecting sovereignty and the need to strengthen cybersecurity capabilities (Devanny & Laudrain, 2025).

(Devanny & Laudrain, 2025) India's policy frameworks, such as the National Cybersecurity Policy of 2020 and the guidelines in the Information Technology Act, provide a structured approach to cybersecurity. Their main objectives are critical information infrastructure (CII) protection, institutional framework and governance, capacity and skill development, cybercrime prevention and law enforcement, public-private partnerships, cybersecurity awareness, and international cooperation. They focus on the following strategic measures: the National Cybersecurity Coordination Centre (NCCC), cybersecurity training and certification, sector-specific Computer Emergency Response Teams (CERTs), research and innovation,

and legislative action (Understanding India's Cybersecurity Policy Frameworks: IT Act, National Cybersecurity Policy, and Strategy, 2025).

India is focused on enhancing its cyber warfare capabilities to counter Pakistan according to regional landscape of South Asia. The cyberspace strategies by India can be utilized as psychological operation and humiliate the competitor in order to achieve political goal at regional as well as international scale. (Ashraf & Ashraf Kayani, 2023)

Cybersecurity has a major influence on the strategic dynamics of the international system and the internal security of several nation states, reflecting and reinforcing the growing importance of cyber operations for these nations. It can be concluded that the frequency and intensity of cyber operations between countries will accelerate. For example, the United States and China are clashing in the field of cyber warfare, which is becoming unpredictable with the introduction of artificial intelligence. Countries' efforts to improve their own security often imply the security of others, which in turn pushes other political actors to take countermeasures. For example, the cyber competition between the United States and China has a direct impact on India's national security. When it comes to cyber capabilities, the perception of an adversary's capabilities is an important element of the overall defensive strength. Therefore, the current model of political and military alliances may need to be redefined to account for cyber competition between allies. The fact that many actors operate in cyberspace or use information technologies shows that the cyber dimension of current international relations is extremely complex and subject to unpredictable developments. As a result, the actions and responses of different countries will influence each other and change the nature of the threat. (Gorka, 2023)

Therefore, non-governmental organizations, leaders and certain international institutions can represent policymakers or participate in the securitization process at the international level. For example, the United Nations can implement securitization by identifying specific issues as "threats to international peace and security." The media is an important platform for conducting such representative actions, both at the national and international levels. One of the main unknowns and difficulties facing policymakers and researchers in international cybersecurity is whether there is a reliable mechanism for attributing cybersecurity incidents. This knowledge is crucial for the development of international law and for determining the responsibility of states for offensive acts in cyberspace. Therefore, cybersecurity policies are highly asymmetric, which makes defense strategies based on specific attributions seem outdated. (Gorka, 2023).

Theoretical Framework

Techno-liberalism

Techno-liberalism is a political and social ideology that incorporates the principles of classical liberalism and emphasizes the transformative potential of technology. This ideology advocates the use of technology to enhance individual freedom, improve governance, and stimulate economic growth, while adhering to

the maintenance of individual freedom, free markets, and limited government intervention. The key elements of the theory include: First, individual empowerment, which gives individuals greater autonomy, access to information, and opportunities for personal and professional development. Second, innovation and entrepreneurship, which believes that technological progress can stimulate economic growth and improve the quality of life. Third, free markets, which advocates that government intervention in the economy should be minimized and encourage competition and market-based solutions to social challenges. Fourth, digital rights and privacy, which advocates the protection of personal information and the right to online privacy. However, data protection regulations should not hinder innovation and progress. Fifth, transparent and accountable governance, which uses technology to create more transparent, efficient, and accountable governance structures, such as through e-government initiatives and digital public services. Sixth, global connectivity supports the idea of global connectivity and the free flow of information across borders, which is believed to promote greater understanding, cooperation, and economic opportunities around the world (Techno Liberalism).

In this way the Techno-liberalism or capitalism provides favorable position to private tech companies as “national champions” who partner themselves with state’s military or intelligence institutions. This allows commodification of Private-Public Partnerships (PPP) in addressing national security and international security paradigms specially in cyberspace. Basically, this militarization of cyberspace where tech firms control the digital technology and security of state by generating discourse of patriotism (Mathur, 2025)

This theoretical framework introduces the concept of classical liberalism into the technological realm, guaranteeing individual freedom in digital spaces. Adam Fish's timely book, "Techno liberalism and the End of Participatory Culture in the United States," examines television as a democratic tool in the struggle for and on behalf of participatory public spheres in the media. In this contested and overdetermined area, Fish presents the concept of techno liberalism as a designation for certain discourses about technology, often accompanied by deregulation that seeks to invalidate the need for participatory politics. Fish describes how these discourses are mobilized to "reduce the contradictions of liberalism itself." By connecting the history of American television to the recent consolidation and monopolization of the internet, Fish shows how democratizing platforms have been assimilated by the logic of capitalism. According to Fish, the internet has transformed from a participatory public sphere into a capitalist enterprise. For example, this might seem somewhat contradictory to Fish's claim that the Internet's potential for participatory politics has been replaced by a "supply-side gold rush."

Security Dilemma Theory

The Security Dilemma Theory was given by British historian Herbert Butterfield in 1949. The term was coined by American scholar John Herz. This theory argues that due to absence of supreme authority in international system, the

circumstances compel states to enhance their own security for survival. As states go for advancing their own capabilities then it creates sense of insecurity in other states. This eventually led to increase chances for arms race and eventually war (Wivel).

The main idea of Realism is focused on power and survival which basically considers cyberspace security as normal extension of conventional security threat. Due to anarchy in the international system states go for enhancing their self-reliance, safety, security and technological developments. Realists argue that cyberspace capabilities ensure the survival of nation and preservation of national interest. The threats of cyber and space security has converted the "low politics" to a matter of "high politics" as it effects state sovereignty and national interest directly (Cavelty, 2019).

But somehow the cyberspace advancement has increased the traditional security dilemma because the cyber and space technologies follow bother offensive and defensive patterns of engagement. The cyberspace advancement of one state is seem as a threat by other state. This actually allows a competition and race to prevail as defensive measures by one state led to offensive reaction by other state which eventually overall creates insecurity. Other than that the prevalence of non-state actors like hackers, and cyber terrorist further complexes the response by the state and its institutions by creating space for preemptive reaction and mistrust more prevalent. In this theoretical framework the for cybersecurity requires power maximization but it also exacerbates the instability, mistrust and competition and creating security dilemma (Arslan).

Securitization Theory

Securitization theory assumes that securitization occurs when actors present political issues as existential threats in their discourse, thus motivating states to act accordingly. The Copenhagen School of securitization theory has been increasingly applied in international security studies in the early 21st century, and its theoretical framework represents an important turning point. Securitization theory focuses primarily on hypotheses and counterfactual arguments about alternative future scenarios. These statements typically contain two predictions: what happens if the securitization measure is not implemented, and what happens if it is implemented? Securitization research is qualitative and comprises three phases of analysis: depoliticization, politicization, and securitization. Its development also requires: (i) the identification of securitizing actors and the discourses they use to socially construct threats; (ii) the analysis of this discourse's ability to convince specific audiences of the threat danger; and (iii) the analysis of the capacity of this discourse to convince specific audiences of the threat danger. and (iii) examining the emergency policies and measures adopted by the state in response to the threat. This means that empirical evidence on securitization requires an analytical roadmap, which, from the researcher's perspective, requires consideration of the securitization discourse and its ability to convince the public of the need for emergency measures. (Viana Silva & Pereira, 2024). (Viana Silva & Pereira, 2024)

At its core, securitization examines how everyday problems are transformed into existential threats. It is like flipping a switch: floods, disease outbreaks, and even economic crises—previously considered serious threats to a cherished "reference point" (whether it be a community, a way of life, or humanity itself)—can trigger extraordinary actions that go beyond the norm. The process studied by Wæver bears striking similarities to the actions of militaries in response to hostile threats. The strength of securitization theory lies in its broad perspective. It goes beyond the state-centric perspective of traditional security studies to encompass issues of global concern. This allows us to analyze non-state actors such as terrorist organizations, transnational threats such as cyber warfare, and even seemingly unrelated issues such as environmental degradation or epidemics. By understanding how these different issues are securitized, we can gain valuable insights into how societies respond to major challenges. In today's complex world, securitization theory is undoubtedly relevant. It allows us to look beyond the surface of threats, unpack their root causes, and analyze the power dynamics involved. (Otukoya, 2024).

The securitization of cyberspace poses a national security problem. This problem is particularly complex for developing countries, where the use of information technology is developing more rapidly than in other parts of the world. With the rapid spread of technologies such as mobile telephony and the Internet, the idea has spread that they can strengthen democracy. Although evidence supports this hypothesis, restrictions on rights and freedoms can also be observed in cyberspace. Countries around the world are increasing their control over cyberspace to ensure that its content is consistent with their national and international political interests. Most academic research on cybersecurity focuses on threats and does not discuss securitization theory. One of the rare exceptions, however, is research that uses the Copenhagen School's securitization theory to analyze cybersecurity discourse and practice. (Gorka, 2023).

Problem Statement

Cyberwarfare between USA and China has become major concern in International Relations, mainly it is creating strategic uncertainty for national security of India. Despite advancement in technological and digital capabilities the cybersecurity architecture of India remains unprepared to counter the major power competition in cyberspace especially with inclusion of Artificial Intelligence.

Purpose of Study

Research Objectives

- To analyze impacts of US-China cyber warfare on national security of India
- To explore affect of India's dependence on foreign alliances and technology
- To assess the use of AI in US-China rivalry and its vulnerability for India
- To analyze India's cyber and space capabilities and available options in lieu of major powers rivalry

Research Questions

- How does the ongoing cyberwarfare between US and China impacts the India's cybersecurity and sovereignty?

- In what way India's dependence on foreign technology and alliance affects its cybersecurity posture?
- What are the vulnerabilities in cybersecurity infrastructure of India in face of AI-powered cyber threats originating from Sino-American rivalry?
- What policy recommendation can strengthen India national security in context of gobal cyber warfare between two major powers.

Nature of Study

This research study incorporates qualitative research to explore AI-driven cyberwarfare between US and China and its impacts on national security of India. It focuses on identifying strategic challenges, cyberspace posture and policy gaps through interpretive lens. The secondary form of research was used with collecting data and information from books, journals, article and documents.

LITERATURE REVIEW

They look at the rising cyber warfare battle between the U.S. and China and explain how it plays a bigger part in both countries' military and geopolitical plans. They maintain that, just as there are land, air, sea and space battles, now we have cyber conflict and both sides are developing modern cyber defenses to have an edge. The paper explains that growing cyber threats are shifting previous security approaches and causing greater global tension. Most experts agree that cyber-attacks are now central to how nations conduct foreign relations and deter enemies. This race in cyberspace, the experts argue, causes instability in international security because there are few clear guidelines or safeguards. The paper gives a clear and complete explanation of cyber command systems and core doctrines which is backed up by carefully arranged figures. The research also covers an essential topic where technology and global politics meet. Even so, the paper draws mainly from second-hand information and does not have any case studies. Furthermore, it does not explore the effects of these issues on regional countries, nor suggest strategies to deal with the new risks (Khn and Abbasi 2023).

The author examines how changes in cyber warfare techniques have influenced global political relations, mainly because of rising competition between the U.S. and China. The paper outlines the increasing presence of military elements in cyberspace, the discrepancy in cyber abilities across nations and the weakness in cyber governance around the world. It also focuses on the ways regional dynamics are affecting South Asia, mainly the changing situation with India and Pakistan's cybersecurity. The author argues that using cyber resources has opened up a new way for countries to influence events. When major nations use cyberspace for attacks, they upset the main principles of military action, boost competition for influence and make it harder to cooperate diplomatically. According to the paper, failing to address cyber norms and governance will increase tension between the U.S. and China, resulting in further challenges for nearby countries like India. This study offers solid comparisons between the cyber policies of the U.S. and China, explains the structure of both countries' militaries and includes information on South Asian

cyber politics. Nevertheless, there is not enough research on important cases and too little exploration of India's AI-related cybersecurity problems. Suggesting specific actions to support regional security when faced with the global cyber arms race would support the paper's main arguments (Firdous, 2020).

This paper brings together and organizes the research on using Artificial Intelligence (AI) to tackle cybersecurity problems. It means AI can support our security by finding breaches, studying software malware and predicting cyber-attacks. They reveal that AI programs are superior to previous methods because they manage massive data and fast-changing dangers found online much better. According to the authors, the evolution of cyber-attacks requires a flexible and reputable defense system. Researchers find that due to machine learning and deep learning, AI creates a quicker response to cybersecurity challenges. This study further explains that AI can detect threats earlier so, that digital platform and interactions can be made safer. The study explains in detail how AI is used for cybersecurity and why certain AI solutions are better than others. Nevertheless, more examples from either research or real situations would increase the credibility of the study's arguments. This article explains benfits of use of AI in cybersecurity however, considering its ethical and moral obligation could make it more balanced (Akhtar and Feng, 2021).

This article focuses on the varied cyber strategic battle between the United States and China, looking at its effects on international politics, the world and technology. The analyze examines how cyberspace plays a key role in shaping security, government power and stability of the world economy. The article explores the cyber capability growth of many countries, increases in cyber warfare threats and any effects on international traditions and diplomacy. According to the authors, this geopolitical rivalry extends beyond conventional military fights to depend on ideology, technology and standards. They argue that this competition is affecting global relations, as both nations use technology, diplomacy and the creation of cyber norms to take control in cyberspace. The paper points out that strategies must take into account the relationship between technology and international politics. The key to the article is its use of both geopolitical knowledge and knowledge of technical matters. It gives a detailed picture of interactions between the US and China in cyberspace. A further discussion of strategies and mechanisms that could provide ways of cooperating or easing tensions might enhance the article practical significance (sing et al., 2025).

This research examines how cybersecurity in India affects national defense and how well existing rules cope with new threats. The authors use a qualitative-descriptive design and thematic content analysis to look through secondary data from government files, think tanks focusing on security and political documents. The paper lists important challenges, primarily in the form of phishing (34.67%), ransomware (25.33%) and cyber espionage (16.67%), most often faced by defense, finance and government sectors. It points out that there are large weaknesses in carrying out policies, combining agency efforts, financial resources and human

capital. According to the authors, the country's fast move to digital has overtaken its defenses, making it more vulnerable to threats against the nation. They highlight that improving cybersecurity involves forming a solid plan to deal with new risks and ready the organization for them. Major steps are to introduce Central Cybersecurity Authority, which provides appropriate cybersecurity training and enhance cooperation with other states. The work contains an in-depth look at the issues and policy problems facing Indian cybersecurity, supporting its approach with established standards from NIST and ISO/IEC 27001. What makes it strong are its analyses of different kinds of threats and how different policies respond to them. Nonetheless, backing up its arguments with more evidence from case studies would improve this work. Going further into the reasons for differences in cybersecurity laws would enrich the study of the subject (Anita and Samal, 2025).

The paper analyzes how cybersecurity is currently positioned in India. Cyber Knights begins by outlining the main ideas behind cybersecurity and the key reason it's now important. The writers mention the most common cyber dangers that confront individuals and organizations in India like phishing, virus by malware and data being stolen or lost. The study also looks at the actions the Indian government has taken, for example setting up CERT-In teams to address and contain cyber incidents. According to the authors, as India progresses with digitization, it is confronted by growing cyber dangers which call for better cybersecurity. They stress that everybody, including businesses and individuals, should keep learning about cybersecurity. The paper adds that a reliable legal structure and international cooperation are critical for stopping cyber-attacks in today's connected world. It clearly describes the important cybersecurity issues in India and details the government's actions to solve them. It demonstrates what the current cyber threat environment looks like and the role of CERT-In. Extra case studies or data from studies could help support and improve the results presented in this paper. In addition, a closer analysis of certain policy actions and how well they function would improve the paper's practical significance (Tejpal and Patole, 2023).

This paper explores the regulatory problems associated with using AI as part of India's cybersecurity. It reveals that existing laws are not fully prepared to handle the special problems that arise with artificial intelligence such as hidden algorithms and adversarial incidents. According to this study proper guidelines are very much important to maintain trust, honesty and encouragement of ethical and moral development in AI. According to Meghwal, India's present cybersecurity laws are not designed for the particular dangers linked to AI applications. He emphasizes that changes in regulation are needed to meet the problems that arise when AI combines with new technologies like blockchain. This paper proposes that experts from the private sector and representatives from government work group to establish measures, determine liability and encourage transparency. The paper makes it clear that India urgently needs specific cybersecurity guidelines for AI. It is strong because it points out what laws are missing and suggest ways to resolve policy-making issues through mutual effort. Still, adding empirical data or case studies would support the

arguments in the study. Further studies of global regulations can give India ideas to improve its laws (Meghwal, 2024).

Findings

The cyber struggle between the United States and China is changing the way India looks at national security. The rivalry between China and India is having major effects on India's cybersecurity, considering how important AI is becoming for cyber actions.

Both countries are now heavily engaging in advanced cyber threats in their conflict with one another. Suspected cyberattacks and espionage from China against U.S. critical infrastructure have encouraged the U.S. to strengthen its cyber security and strike power. The escalation in cyber-attacks leads India and similar countries to focus on their cybersecurity, prepared for the negative impacts and risks for their essential structures.

India is currently in a vulnerable situation because it is regularly attacked by state and non-state cyber actors. Defense, financial and healthcare sectors in the country have seen an increase in cyberattacks. The Operation Sindhoor case also revealed that pro-India hacker groups are essential in stopping cyberattacks from neighboring countries, making it clear that a strong and unified cyber defense approach is needed.

AI is being seen as both a tool and a threat in security against cyber-attacks. First, these tools increase how threats are found, respond automatically and anticipate future risks. If you look at it differently, adversaries also make use of AI to design more advanced threats, for example, deepfakes and computer programs that use AI. India is just start with AI use in cybersecurity and organizations such as the AI Safety Institute are working to make it safe.

India's rules regarding AI and cybersecurity are being updated. The passing of the Digital Personal Data Protection Act, 2023 is an important advance in protecting people's privacy. But experts believe that modern laws are not sufficient to deal with the challenges caused by AI. The Digital India Act seeks to create a more complete set of laws, though how it will be used and how effective it is has still not been observed.

Given that cyber threats often affect countries worldwide, India has started working with other nations to grow its cybersecurity. As an example, the United States–India Initiative on Critical and Emerging Technology (ICET) is concentrating on working together on AI, quantum computing and cybersecurity. They are important because they share knowledge and help create safe cyber networks.

Despite understanding that AI can improve cybersecurity, India is encountering issues with implementing AI. A key reason is the lack of experts capable of handling AI and cybersecurity together. It is tough for technology companies to get AI-driven security tools approved because of a lack of infrastructure. New rules on surveillance also cause delays in approvals.

India should engage in several actions to deal with the influence AI, cybersecurity and geopolitics play: making sure existing laws are updated to include

AI-related things and defining clear regulations for cybersecurity. Training and teaching to make the workforce skilled at controlling AI systems used for cybersecurity. Working more closely with partners around the world to share experiences, information and assets. Ensure that government agencies and the private sector collaborate to bring about innovation, but also to secure systems unity.

Recommendations

As cyber warfare between the United States and China grows, India faces its direct implications. To navigate this complexity a multifaceted approach is required like given more digital risks, strategic significance in the Indo-Pacific and enhanced use of Artificial Intelligence (AI), defenders in India should quickly update their cybersecurity approach.

Prepare an Integrated AI-Cybersecurity Law Incorporating Risk-Focused Provisions

India should put in place a law that both covers uses of AI and ensures cybersecurity. According to Carnegie Endowment (2024), the Digital Personal Data Protection Act is not adequate to address algorithmic bias, data misuse or independent cyber-attacks. The Digital India Act should clearly govern the use of high-risk AI in fields like defense, finance and offices of the government.

Reference: Carnegie Endowment (2024) – India's Advance on AI Regulation

Put a National Cybersecurity Command into practice.

So far, the concept of a central agency for cybersecurity, suggested in many strategic discussions, has not been put into practice. To ensure good response, coordination, ethical testing and active cyber defense, an AI-led Cybersecurity Command should come under the Ministry of Home Affairs or Defense. The body would use offensive weapons in a lawful system under proper checks and controls.

Develop a cyber policy that allows the country to act with autonomy.

According to Carnegie, the country does not have a written cyber doctrine that outlines what it hopes to achieve, how it will deter and the policies it will follow. As the tension in cyberspace between the United States and China has added much confusion such a doctrine can deliver clarity. Its control must consider how automation can work in harmony with cooperation between countries in cyberspace.

Support more AI research and development within troops and cyber units.

Most of India's AI growth is now tied to foreign technology. The idea shared by NASSCOM and ORF is that cooperation between public and private entities will increase Indian control over AI and lessen the need for foreign technology. The DRDO and private sector should help initiate a national mission on AI in Cyber Defense.

Defend Critical Infrastructure more effectively by using AI.

A new approach to security is needed besides using only firewalls to protect critical infrastructure. The NDU Journal and PIB suggest that predictive analytics, anomaly detection and a zero-trust approach are needed in India. Under the law, CII operators should conduct AI-based threat intelligence and cyber simulated events at least every three months.

Form a board that will oversee cyber ethics and artificial intelligence.

As a means of reducing ethical risks in using AI for surveillance and military, India should create an independent overseeing group made up of technologists, experts in law, competent members of civil society and defense planners. It would be responsible for examining whether a country's AI is aligned with ethics, is unbiased and respects human rights.

Help More People Get Training in Cybersecurity and AI

A shortage of trained staff is making India's digital defense less effective. Experts at Modern Diplomacy and NASSCOM point out that launching a cyber-literacy program should be a national goal. Scholarships, collaborations with industry and AI-for-cyber bootcamps should be introduced in Tier-2 and Tier-3 cities to create a larger group of IT professionals.

Improve the way cyber topics are handled on regional and global levels.

India needs to take a greater role in shaping cyber norms around the world. The UN's OEWG on Cybersecurity and the Global Partnership on AI serve as good places for India to counter both the U.S. and Chinese roles. Cooperation in the Indian Ocean region and East Asia will further decrease cyber reliance.

Require AI-Explainability and Proper Redressal in Government Systems

As AI takes on greater importance in digital governance, people must be able to see how AI-related decisions are formed. AI used for governance and security of a nation should be easy to read and review. So, India should formally enact and enforce these OECD and UNESCO standards.

Foster Public Awareness and Cyber Hygiene

It is important to educate people on cyber security to protect the digital world. Create campaigns that warn people nationwide about possible dangers from AI and provide them with recommendations. Cybersecurity knowledge should be introduced early in children's education.

Strengthen Engagement in Global Cyber Norms Forums

India needs to participate actively in global cyber forums to help create new rules and lower its risk in an era when U.S.–China cyber rivalry is growing. India could help decide how nations behave responsibly in cyberspace by being actively involved in the UN OEWG and the GFCE. Taking part as an observer in the Budapest Convention might improve India's legal ability to deal with international cyber offenses.

Build cyber trust and joint resilience through strategic forums

Platforms like QUAD Critical and Emerging Technologies Working Group and the IPEF provides nations in Indo-pacific to establish and discuss AI standards and ethics, securitize digital frameworks and flow of information. Such forums provide an opportunity for India to establish trust and resilience with similar democracies throughout the Indo-Pacific. In cybersecurity and AI, India should strengthen its efforts with the United States under iCET and add similar approaches to its deals with the European Union, Japan, Israel and Australia. India can use these agreements to boost cybersecurity, encourage fair AI growth and create closer

international relations for the purpose of challenging U.S. and Chinese leadership in cyberspace.

REFERENCES

Adegbite, A. O., Akinwolemiwa, D. I., Uwaoma, P. U., & Kaggwa, S. (2023). REVIEW OF CYBERSECURITY STRATEGIES IN PROTECTING NATIONAL INFRASTRUCTURE: PERSPECTIVES FROM THE USA. Retrieved from https://www.researchgate.net/publication/376807006_REVIEW_OF_CYBER SECURITY_STRATEGIES_IN_PROTECTING_NATIONAL_INFRASTRUCT URE_PERSPECTIVES_FROM_THE_USA

Akhtar, M. S., & Feng, T. (2021). An overview of the applications of Artificial Intelligence in Cybersecurity. EAI endorsed transactions on creative technologies, 8(29).

Arslan, A. (n.d.). Neorealist Analysis of Security Dilemma in Cyberspace; A Quantitative Study. Retrieved from https://preprints.apsanet.org/engage/api-gateway/apsa/assets/orp/resource/item/6426247691074bccd08fc239/original/neorealist-analysis-of-security-dilemma-in-cyberspace-a-quantitative-study.pdf

Ashraf , N., & Ashraf Kayani, D. (2023). Indian Cyberwarfare capabilities: Repercusssions for Pakistan's National Security. Retrieved from https://ndujournal.ndu.edu.pk/site/article/download/152/114

Cavelty, M. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Retrieved from https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1678855#abstract

Devanny, J., & Laudrain, A. (2025). Interpreting India’s Cyber Statecraft. Retrieved from https://carnegieendowment.org/research/2025/03/interpreting-indias-cyber-statecraft?lang=en

Firdous, M. A. (2020). Cyber Warfare and Global Power Politics. CISS Insight Journal, 8(1), P71-93.

Gorka, M. (2023). Conceptualizing Securitization in the field of Cybersecurity Policy. Retrieved from https://www.jomswsge.com/pdf-176103-98736?filename=Conceptualising.pdf

Huang, T. (n.d.). Research on Cyber Space Security Strategy of the United States. Retrieved from https://www.atlantis-press.com/proceedings/iafsm-18/55915228

Khan, S. A., & Abbasi, S. N. (2023). The US-China Cyber Warfare in the 21 st Century. Insight Turkey, 25(2), 163-186.

Knight, S. (2015). Cyberspace with Chinese Characteristics. Retrieved from US Naval Institute: https://www.usni.org/magazines/proceedings/2015/april/cyberspace-chinese-

characteristics

Meghwal, T. (2024, September 4). Emerging challenges in regulating Artificial Intelligence under cyber security laws in India. SSRN. https://doi.org/xxxxx (replace with actual link or DOI)

Mathur, R. (2025). Techno-Capitalism and Weaponization of Cyberspace. Retrieved from https://academic.oup.com/isagsq/article/5/2/ksaf031/8108262

Otukoya, T. (2024). The Securitization Theory. Retrieved from https://ijsra.net/sites/default/files/IJSRA-2024-0225.pdf

Techno Liberalism. (n.d.). Retrieved from https://technoliberalism.org/

The State Council Information Office of the People's Republic of China. (2023). Retrieved from Full text: China's Law-Based Cyberspace Governance in the New Era: http://www.scio.gov.cn/zfbps/zfbps_2279/202303/t20230320_709283.html

Tejpal, K., Vidyapeeth, D. P., Pimpri, P., & Patole, J. (2023). Cybersecurity: Pressing priority in India. The Online Journal of Distance Education and e-Learning, 11(2), 2052-2061.

Singh, N. K., Jash, A., & Nanjappa, Y. (2025). Navigating the nexus: geopolitical, international relations and technical dimensions of US-China cyber strategic competition. Cogent Social Sciences, 11(1), 2499171.

Sunita, & Samal, A. (2025). Cyber threats and national security in India: Evaluating policy measures and emerging challenges. International Journal of Political Science and Governance, 7(1), 232–240.

Toma, P.-S. (2024). An Overview of China's Development in Cyberspace. Retrieved from https://www.researchgate.net/publication/385391583_An_Overview_of_China's_Development_in_Cyberspace

Understanding India's Cybersecurity Policy Frameworks: IT Act, National Cybersecurity Policy, and Strategy. (2025). Retrieved from https://www.rsm.global/india/insights/consulting-insights/cybersecurity-policy-frameworks

US Department of State. (2025). Retrieved from United States International Cyberspace & Digital Policy Strategy: https://2021-2025.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/

Viana Silva, C., & Pereira, A. (2024). Securitization theory and its empirical application: a literature review. Retrieved from https://www.scielo.br/j/rsocp/a/StyctPjZ4t7Dr9kkDNHkq9L/

Wivel, A. (n.d.). Security Dilemma. Retrieved from https://www.britannica.com/topic/security-dilemma