

United states, China and the role of CISA (Cybersecurity and infrastructure security agency)

Faisal Hayat¹

Abstract

The escalating cyber rivalry between the United States and China marks a defining feature of modern geopolitical conflict, with cyberspace emerging as a boundless battlefield targeting national infrastructure and digital sovereignty. This study explores the evolving cyber dynamics with a focus on the U.S. Cybersecurity and Infrastructure Security Agency (CISA), highlighting its strategies to counter cyber threats, particularly from China. These threats range from state-sponsored espionage to infrastructure attacks, with over 20,000 incidents targeting U.S. critical systems in 2023 alone. Established in 2018, CISA plays a central role in securing national cyber resilience and coordinating responses across sectors. Through qualitative case studies, policy analysis, and thematic review, the research assesses CISA's operational responses—such as during the 2021 Colonial Pipeline attack—and its partnerships with government, private, and international actors. It also identifies institutional limitations and strategic gaps. This paper underscores the importance of domestic institutional readiness in addressing global cyber threats, advocating for adaptive governance, increased investment, and international cooperation. CISA is portrayed not merely as a reactive entity, but as a strategic asset in the United States' digital defense architecture.

Keywords: CISA, cyber warfare, U.S.-China rivalry, cybersecurity policy, digital infrastructure, critical infrastructure protection, cyber resilience, national security, cyber geopolitics

Introduction

In 2023 alone, the U.S. faced over 20,000 cyberattacks targeting critical infrastructure, many of which were attributed to China (CISA, 2025; Politico,

¹ Department of Political Science & International Relations, University of Management and Technology, Lahore - Pakistan

2025). These attacks were not merely economic disruptions but compromised hospitals, energy grids, and financial institutions. As international cyber threats intensify, one critical question arises: How prepared is the U.S. to defend its cyberspace?

The virtual battlefield between superpowers such as the United States and China grows increasingly complex. As China rapidly expands its cyber capabilities and engages in state-sponsored cyber espionage (Lindsay, Cheung, & Reveron, 2015), the U.S. faces mounting pressure to secure its national infrastructure. At the forefront of this defense is the Cybersecurity and Infrastructure Security Agency (CISA), which plays a central role in mitigating cyber threats through collaboration with public and private sectors and disseminating threat intelligence.

Cyber warfare, once seen as a purely technical domain, has now become a critical dimension of national security and international politics (Casey, 2022). While the U.S. has historically emphasized conventional military strength, its digital defenses have lagged behind. The formation of CISA in 2018 marked a turning point, centralizing cyber defense strategy under the Department of Homeland Security (DHS).

When cyber systems fail, millions of Americans are affected—from hospitals unable to access medical records to gas stations losing digital payment systems. These attacks cost billions of dollars and erode public trust. If CISA can successfully mitigate such threats, the U.S. could emerge as a global leader in cyber defense.

Although the broader U.S.-China cyber tensions have been well-documented (Li & Zhu, 2017), limited attention has been given to how CISA fits into the strategic equation. While China's digital strategy is increasingly understood, CISA's evolving role requires deeper investigation.

Real-world indicators reveal the urgency: in 2023, 75% of U.S. critical infrastructure operators reported cyber incidents (CISA, 2025). Resource constraints further complicate matters, with CISA Director Jen Easterly warning of an impending "moment of reckoning" (Politico, 2025).

A notable case in point is the 2021 Colonial Pipeline ransomware attack. CISA's swift response underscored its role in managing national-level cyber emergencies.

This paper examines the strategic role of CISA in countering cyber threats from China. It draws on policy analysis, case studies, and expert commentary to assess how CISA is shaping national cybersecurity policy and international cyber relations.

Through initiatives like the Joint Cyber Defense Collaborative (JCDC), CISA integrates federal agencies and private companies to improve real-time threat detection. Training programs, public awareness campaigns, and risk management protocols highlight CISA's transition from a technical division to a national cyber command center.

Literature Review

The study examines the escalating cyber competition between the United States and China with a focus on the strategic and operational significance of the Cybersecurity and Infrastructure Security Agency (CISA) in U.S. cybersecurity policy. The research adds to the body of literature by identifying the geopolitical and institutional aspects of cyber threats and national response mechanisms (Carr, 2016; Klimburg, 2017).

❖ Geopolitical Cybersecurity Dynamics

There is a large body of research that has addressed the geopolitical rivalry between the United States and China in cyberspace. Researchers have chronicled the ascendance of state-sponsored cyber espionage, the targeting of strategic infrastructure, and the use of cyber capabilities as tools of state power (Lindsay et al., 2015; Sanger, 2018). The paper extends this base by situating cyber warfare in the broader context of international relations and national security policy as a core issue, rather than simply as a technical problem. In contrast to other studies that are primarily concerned with state actions or diplomatic consequences, this research places CISA as a key institutional agent in addressing these threats (Healey, 2013).

❖ The Evolving Role of CISA

The study contributes to an increasing body of work that examines U.S. domestic cybersecurity policies. CISA, which was created in 2018 under the Department of Homeland Security, is referred to as the front line of defense against cyber assaults (CISA, 2025). Writing about institutional cybersecurity in the U.S., literature tends to refer to CISA in broad terms; this article delves deeper into its precise roles, including public-private partnership, coordination with other federal agencies, and

live threat evaluation (Politico, 2025). It highlights the agency's proactive and responsive abilities through instances such as the Colonial Pipeline ransomware attack, thus contributing to arguments of the agency's growing relevance in managing cyber crises.

❖ **Infrastructure Vulnerabilities and Incident Response**

Current literature has identified weaknesses in critical infrastructure like healthcare, energy, and finance (Knake & Rattray, 2016). The article confirms these allegations using real-world data—for instance, indicating that 75% of critical infrastructure operators in 2023 had cyber-attacks (CISA, 2025). It also adds to the academic literature by probing the effect of such weaknesses on national resilience and public confidence, areas less focused in previous research.

❖ **Shortcomings and Criticisms of CISA's Capacity**

A number of scholars and policymakers have raised an eyebrow regarding the ability of CISA to meet its expanding mandate. The article recognizes this through the provision of critical perspectives regarding resource limitations and the magnitude of CISA's roles (Casey, 2022). Although previous studies at times neglect institutional capacities, this article strikes a balance between optimism regarding CISA's mission and an honest analysis of its limitations.

❖ **Conclusion of Literature Positioning**

This research adds depth to academic discourse by combining policy analysis, case studies, and strategic assessment of cybersecurity governance. It fills an evident gap in the literature since it directly explores the manner in which a single U.S. agency—the CISA—manages the multifaceted environment of cyber threats from a global superpower such as China. The research opens space for additional scholarly investigation on institutional effectiveness, global cooperation on cyberspace, and responsive cybersecurity policymaking.

Methodology

This study employs a qualitative, exploratory research design to analyze the emerging cyber competition between China and the United States and the strategic function of the Cybersecurity and Infrastructure Security Agency (CISA) in responding to cyber threats. The research is mostly descriptive and analytical,

seeking to evaluate current policies, actual cyber events, and institutional mechanisms instead of hypothesis testing via empirical or quantitative means.

❖ **Data Sources**

The study relies on a mixture of secondary sources of data, including:

- CISA and the U.S. Department of Homeland Security policy documents and government reports.
- News reports and expert commentary concerning cyberattacks, particularly those attributed to China.
- Scholarly publications, think tank reports, and journal articles on cyber warfare, critical infrastructure, and cybersecurity policy.
- Case studies, specifically the 2021 Colonial Pipeline ransomware incident, are utilized to demonstrate CISA's contribution to real-time cyber crisis management.

❖ **Analysis of Case Studies**

A key aspect of the methodology is the application of case studies, specifically instances of U.S. critical infrastructure attacked that have been attributed to foreign cyber actors. These cases shed light on:

- The extent and nature of cyber threats.
- CISA's response operations.
- Policy implications and institutional constraints.

❖ **Review of Policy and Content Analysis**

Content analysis of strategic reports and cybersecurity policy designs is used in the study. Such key documents as national cybersecurity strategies, interagency coordination policies, and public-private partnership models propagated by CISA are reviewed.

❖ **Thematic Focus**

The research is structured around themes of focus:

- China's cybersecurity threats.
- The institutional capacity and role of CISA.
- Vulnerabilities in critical infrastructure.

- National cyber defense and resilience mechanisms.

❖ **Limitations**

This study is constrained by the use of secondary data, which can be incomplete or biased. Also, classified or restricted data on individual cyber incidents or U.S. cyber defense procedures are outside the purview of this investigation. The analysis also concerns itself mainly with U.S. viewpoints, without much access to Chinese government sources or internal cybersecurity policy information.

❖ **Findings**

Escalating Chinese Cyber Threats: The study points to a sharp rise in cyber-attacks on U.S. critical infrastructure, with most of the attacks allegedly attributed to state-sponsored actors in China. The United States alone was subjected to more than 20,000 cyber-attacks in 2023, affecting vital services including hospitals, the energy grid, and financial systems. This reflects China's expanding capacities in cyber warfare and espionage.

CISA's Critical Role in U.S. Cyber Defense: The Cybersecurity and Infrastructure Security Agency (CISA) has been a focal point in the U.S. fight against cyberattacks. The research discovers that CISA:

- Coordinates national cyber responses.
- Works hand-in-hand with both government and private industries.
- Has a significant role to play in securing critical infrastructure?

Its move in major incidents—like the 2021 attack on Colonial Pipeline—is a clear indicator of its operational salience and increasing institutional relevance.

Vulnerabilities in Critical Infrastructure: The report shows that 75% of U.S. critical infrastructure operators had cyber events in 2023 that exposed severe vulnerabilities. Those weaknesses threaten not only digital networks but also public services, economic stability, and national security.

Resource and Capacity Gaps: Though CISA is a crucial part, the research also discovers institutional constraints, such as fear about inadequate funding, staff, and technological assets. Officials and experts—like CISA Director Jen Easterly—admit a possible "moment of reckoning," cautioning that the agency might not be properly positioned to address the scale and sophistication of contemporary cyber risks.

Policy Innovation and Global Cooperation: The study highlights the requirement for continuous innovation in cybersecurity policy and greater international cooperation. Cybersecurity is not an issue to be handled by any one country anymore; it requires global norms, collective intelligence, and strategic partnerships to grapple with transnational threats.

Insufficient Focused Academic Attention on CISA: The article finds a gap in the literature, in the sense that while there has been much literature on U.S.-China cyber rivalry, comparatively less work has been done on CISA's changing role. The research helps bridge this gap by examining CISA's institutional structure, its collaborations, and its reaction mechanisms.

These results cumulatively highlight the multifaceted nature of cyber defense in great power competition, and they support the need to build stronger national institutions such as CISA while promoting international cyber governance.

Discussions

❖ Addressing the Role of CISA in US-China Cyber Competition

The cyber competition between the United States and China is a paradigm shift in world power relations, with cyberspace emerging as an essential domain of strategic competition. This research emphasizes the role of the Cybersecurity and Infrastructure Security Agency (CISA) in national cyber defense and outlines various challenges and opportunities in the existing cybersecurity environment.

❖ CISA's Growing Role and Institutional Challenges

CISA is now the focal point of the cyber defense strategy of the United States. Its role varies from early warning of threats and coordination to response and recovery in the event of a cyber-attack. For example, during the 2021 Colonial Pipeline ransomware attack, CISA coordinated a swift, unified federal response, showcasing its capability to handle country-scale digital disasters. However, despite its increasing responsibilities, CISA faces critical institutional constraints, including limited budgets, difficulty in hiring cybersecurity experts, and bureaucratic delays. These limitations could hinder its ability to respond to increasingly sophisticated cyber threats.

❖ **The Changing Nature of Cyber Threats**

Conventional warfare is being supplanted by quieter and less traceable cyberattacks. In contrast to traditional military threats, cyber intrusions—particularly those linked to Chinese state-sponsored attackers—tend to target espionage or pre-positioning and not necessarily direct destruction. This type of cyber aggression muddles the border between peace and war, making it more difficult to implement classic deterrence or international law. The research determines that these attacks are persistent and frequently go unnoticed for months, making response strategies more challenging.

❖ **Critical Infrastructure at Risk**

Perhaps the most stunning revelation is that 75% of critical infrastructure operators in the U.S. saw major cyber incidents in 2023. Industry sectors including healthcare, energy, and finance are particularly at risk. These attacks pose a risk not only to service delivery but to public safety and economic stability as well. As most of the critical infrastructure belongs to the private sector, a partnership approach—where CISA provides technical assistance and advice and private players deploy effective defenses— is necessary in order to secure national cybersecurity.

❖ **Policy Gaps and Coordination Issues**

Though the 2022 National Cybersecurity Strategy has been released, there are still significant coordination issues among U.S. agencies such as CISA, NSA, FBI, and U.S. Cyber Command. They have duplicated duties and uncertain legal regimes that sometimes hinder information sharing and response during cyber crises. The research recommends that reforms akin to the "Goldwater-Nichols Act," which enhanced coordination in the conventional military domain, are necessary to enhance cyber operations between agencies.

❖ **The Need for International Cooperation**

Because of the global and borderless character of cyber-attacks, international cooperation is important. The research advises creating norms, confidence-building measures, and even bilateral talks with competing states like China. Measures like formal agreements not to attack hospitals or emergency systems can lower the risk of escalation and facilitate responsible state behavior in cyberspace.

❖ **Scholarly Contribution and Conclusion**

This study adds to the emerging field of cyber policy by examining institutional responses and not solely technical ones. It demonstrates that a country's cyber power is based on the functioning of its institutions. In conclusion, the research highlights that cybersecurity is not merely a technical matter but is a core element of contemporary geopolitics and national resilience in the digital era.

The virtual battlefield between China and the United States is fast becoming the hallmark of contemporary geopolitical rivalry. Since cyber threats are increasingly becoming more frequent, sophisticated, and damaging, it is clear that national security no longer resides within physical boundaries but stretches into the realm of cyberspace as well. The importance of the Cybersecurity and Infrastructure Security Agency (CISA) is thus underscored as a front-line guardian in the cyber defense posture of the United States.

The report shows that CISA is at the forefront of safeguarding critical infrastructure, leading national responses, and cultivating public-private collaborations to enhance cyber resilience. Yet, the magnitude of threats—particularly those linked to Chinese state-sponsored actors—is a cause of major concern regarding the preparedness and ability of American institutions. Although CISA has been successful in managing large-scale incidents such as the attack on the Colonial Pipeline, it still experiences difficulties in funding, personnel, and quick flexibility.

In addition, the study emphasizes the imperative for continuous innovation, more robust policy mechanisms, and enhanced global cooperation. The evolving, borderless character of cyber conflict demands an all-domain strategy that integrates technology, strategy, diplomacy, and institutional capability. CISA needs to continually adapt in order to get ahead of the adversaries who use vulnerabilities not only for disruption, but for strategic effect.

In summary, CISA is not merely a federal agency but a linchpin in the United States defense architecture. Its success will be contingent on continued investment, cross-sector coordination, and proactive cyber governance in an age of increasing global cyber competition.

References

-
- Carr, M. (2016). *US power and the internet in international relations: The irony of the information age*. Palgrave Macmillan.
- Casey. (2022). *Cybersecurity Policies of the United States: An Analysis of Political and National Defense Motivations Influencing Its Constant Development*. Retrieved from <https://www.proquest.com/openview/74b8ab29f6of9d2doas59380d4458b1ba/1?cbl=18750&diss=y&pq-origsite=gscholar>
- CISA. (2025). *CISA Live! Presents People's Republic of China Cyber Threats*. Department of Homeland Security.
- Healey, J. (2013). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.
- Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace*. Penguin Press.
- Knake, R. K., & Rattray, G. J. (2016). *Bridging the National Cybersecurity Strategy Gap: The Need for a Strategic Framework*. Council on Foreign Relations.
- Li, A., & Zhu, H. (2017). *Comparison and Analysis of the Legislation on Cyber Security between China and the US*. In *International Academic Conference Proceedings*. Retrieved from <https://americanscholarspress.us/conferences/pdf/IALL2017.pdf#page=159>
- Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (2015). *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press.
- Politico. (2025). *CISA Live! Presents People's Republic of China Cyber Threats*. Retrieved from <https://www.politico.com>
- Sanger, D. E. (2018). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Crown Publishing.

Article Information:

<i>Received</i>	8-Apr-2025
<i>Revised</i>	30-May-2025
<i>Accepted</i>	10-Jun-2025
<i>Published</i>	15-Jun-2025

Declarations:

Author's Contribution:

- **Conceptualization, and intellectual revisions**
- **Data collection, interpretation, and drafting of manuscript**
- The author agrees to take responsibility for every facet of the work, making sure that any concerns about its integrity or veracity are thoroughly examined and addressed

• **Conflict of Interest:** NIL

• **Funding Sources:** NIL

Correspondence:

Faisal Hayat

faisalkhan@gmail.com
