

USA and China: A Comparative Analysis of Cybersecurity Strategies



Muhammad Ibtasam
Ali Shah

PhD Scholar (International Relations), University of Central Punjab, Lahore
ibtaxam@gmail.com

Abstract: *The global interconnection requires nations to build strong cybersecurity strategies because both digital threats and cyberspace are establishing themselves as determinants of national power. The research conducts a detailed comparison between the cybersecurity strategies of China and the United States. The research examines separate political ideologies and economic requirements and cultural elements which shape how each country approaches cybersecurity through diverse policy materials and academic literature and case examples. The analysis investigates how America and China protect their digital infrastructure through different cybersecurity approaches and what the international security consequences are. What possible ways for cooperation and potential cyber conflicts are available? The United States advances a free internet system which requires collaborative stakeholder engagement, advance threat mitigation capabilities, and alliances with international entities to support technological development together with digital accessibility. China supports cyber sovereignty by implementing strict state control and native technological development and extensive electronic surveillance of all its territory. The research aims to give important knowledge that will help officials together with cybersecurity experts and academic scholars strengthen worldwide digital resilience while directing future cybersecurity policy advancement.*

Keywords: USA, China, Cybersecurity, digital warfare, Cybersecurity Strategies, Comparative-Analysis

Introduction

The role of cyberspace has grown significantly since digital transformation because it serves now as a central domain where countries express power international relations and fight for economic advantages. Every societal feature today depends on digital foundations which have made cybersecurity the top national priority for every nation worldwide. International political environments now push countries to establish total cybersecurity defenses which create new norms to regulate digital space. The two major players in the cybersecurity field show contrasting approaches because their political beliefs and economic needs and cultural background are profoundly different. Since its rise as a technological leader

America defends an open internet structure which promotes expression freedom and business-based progress together with collaborative practices. American cybersecurity approaches integrate basic concepts of open communication and combined efforts between public entities and the private sector. The National Security Agency (NSA) along with U.S. Cyber Command maintains partnerships with corporations including Google, Microsoft, and Cisco to build sophisticated defense capabilities and distribute cyber intelligence for implementing secure protection systems. The United States aims to boost economic innovation while upholding its rules-based international role through open digital systems which also advance economic growth and

technological development (Goodman 2016, Broeders & van den Berg 2020). The decentralized architecture supports open information exchange between borders and stakeholders work together to achieve security (Kshetri 2013; Scherer 2018) while the model embraces a decentralized digital system. China bases its cybersecurity policy on state-controlled principles of cyber sovereignty together with government oversight. The Chinese government adopts its cybersecurity approach because it needs to stabilize its internal conditions while keeping social order and safeguarding its political framework. Through strict government oversight and extensive content management the Cyberspace Administration of China (CAC) and other entities exercise control over Chinese cyberspace (Shia, 2015; Tan & Sayankina, 2023). China maintains cyber sovereignty through an overall strategy which works to control bordering information flows because it seeks to keep digital content faithful to national objectives and cultural norms. China has spent significant resources to establish homegrown cybersecurity expertise to develop a defensive-offensive cyber operational framework which operates independently from foreign technology (Kim, 2018; Yu, 2019). These successful defensive measures for secured internal digital domains create global governance questions about international cyber relations and future international cyber relationships. The U.S. and China operate with fundamentally different cybersecurity methods because their political systems and cultural frameworks stand as the root causes for this separation. The American democratic system which operates with free market principles supports an innovative system that progresses through market competition and social contributions. The openness to share resources and information between sectors strengthens economic growth and distinct technological progress according to Lindsay (2014) and Patton (2016). Because of its authoritarian political system China achieves quick implementation of policies along with unified command which allows the state to take controlling measures on digital communication activities. The centralization of cyber powers enables China to maintain stability and expand

its position as a major cyber competitor around the world (Huang, 2016; Li, 2018). The distinct cybersecurity strategies between nations produce a wide array of international effects with advanced consequences. The open framework based on multilateral cooperation used by the United States supports the development of an international digital paradigm that promotes creative input and intellectual exchange. The distributed approach of the open internet provides several vulnerabilities because attackers can use its connectedness to create intricate challenges in threat detection and response (Anderson, 2016; Baker, 2019). The Chinese strategy builds an enclosed digital system under state supervision while creating uncooperative national cyber domains which undermines the worldwide network infrastructure. The split between digital domains makes it more difficult to establish global cybersecurity norms which would weaken international economic stability together with security levels (Johnson, 2017; Kolodii, 2020). Research studies now emphasize the need for comprehensive studies regarding these two opposing digital policy approaches. Research literature points out that America focuses its approaches on maintaining technological dominance through research and defense while China primarily uses its strategies for domestic security control and develops national innovative systems to break free from foreign technology links (Shia, 2015; Yu, 2019; Goodman, 2016; Scherer, 2018). The worldwide cybersecurity realm transforms due to new technology developments including quantum computing along with artificial intelligence and Internet of Things that create growing challenges and possibilities for both countries (Martinez, 2017; Nguyen, 2018). Modern technological developments demand regular updates to national cybersecurity plans because they reveal the need for analytical systems that unite politics with economics and cultural factors. The research examines three main questions regarding digital infrastructure defense methods and cyber sovereignty regulation between China and the United States under this complex political environment. The various security strategies between the United

States and China create fundamental global changes across international safety and digital control functions while influencing the possible outcomes of cyber conflicts and partnerships. This research examines different cyber strategies of both nations to determine their effectiveness while establishing potential global cyber projections. This paper adopts and extends the extensive existing research about national cybersecurity strategies presented in Assoudeh (2020), Cai (2016), and Jacuch (2021) yet establishes a comparative framework to bridge critical gaps in understanding. The analysis applies Cybersecurity Theory alongside Realism and Constructivism to study how states behave in cyberspace through their material capabilities and ideational influences according to Patton (2016) and Kshetri (2013). The introduction subtly connects to existing studies before presenting a specific discussion about how U.S. and Chinese approaches to cybersecurity differ. Digital threats currently enforce a meaningful need for major powers to understand and compare their cybersecurity strategies because they continuously transform international boundaries. The investigation enables comprehensive evaluation between U.S. and Chinese cybersecurity measures while revealing their wider effects on international governance and economic protection and computational combat patterns. The research findings establish themselves as a foundational tool for policy experts and cybersecurity specialists and academic experts who need to develop resilient digital security measures.

What Is Security?

Security exists as the status where people together with institutions and governments lack any form of danger or damage in their environments. Safety perspectives of earlier times mainly concentrated on guarding tangible resources as well as borders. Modern security practice requires protection of three essential non-physical domains including information systems and critical infrastructure as well as the digital environment (Anderson, 2016; Baker, 2019). Current security systems combine physical safeguards and cyber protection mechanisms to defend the unbroken nature and

full function and confidential status of data despite rising security hazards (Smith, 2018; Davis, 2018).

What Is Cybersecurity?

Digital environments require a focused approach in order to implement security principles which results in cybersecurity. The primary mission of cybersecurity is to defend computer systems along with their networks and stored data against unauthorized breaches and cyber attacks as well as digital threats. The foundational principles—the confidentiality, integrity, and availability (CIA) triad—guide both technical and organizational measures (Peterson, 2017; Clark, 2015). The application of encryption alongside secure coding practices and firewalls develops with detection systems using intrusion detection and continuous monitoring tools to make up multiple defense layers (Thompson, 2017; Roberts, 2018). Cybersecurity demands perpetual modifications because novel security threats constantly emerge from updates in quantum computing and artificial intelligence (Martinez, 2017; Nguyen, 2018).

What Are Cybersecurity Strategies?

Digital infrastructure protection requires complete systematic strategies which protect networks systematically. Such plans integrate a combination of connected elements into their structure.

Risk Assessment and Management:

Security methodologies commence with threat and vulnerability detection then use threat intelligence and risk assessment results to develop specific defensive measures according to Lee (2019) and Garcia (2020).

Preventive Measures:

Firewalls and anti-virus systems along with safety compliance protocols work together with network architecture models to defend against cyber threats (Wang, 2021; Zhao, 2021).

Detection and Monitoring:

Through continuous monitoring and invasive systems and analytically empowered detection mechanisms organizations can expedite the recognition of irregularities and data

infringement attempts (Patel, 2020; Davis, 2018).

Incident Response and Recovery:

Incident response plans with clear definitions allow both attacks' containment and operation restitution with reduced interruption (Sun 2020; Li 2018).

International Cooperation and Collaboration:

When addressing cyber threats which span international borders society needs multilateral agreements and public-private partnerships that let partners exchange information to build joint responses (Chen, 2017; Huang, 2016).

Capacity Building and Innovation:

Organizations that make cybersecurity research investments develop skilled employees and create innovative methods and enduring capabilities for defense (Yu, 2019; Kim, 2018). The combination of components in integrated frameworks makes countries stronger in their ability to deal with present and emerging digital threats according to Zhao (2019) and Anderson (2016).

Cybersecurity Strategies Used by the United States

The United States follows an attractively open cybersecurity strategy based on innovation together with collaborative national defense principles. Key elements include:

Open Internet Model and Innovation

The United States defends an open internet system which promotes free expression and generates innovation and stimulates economic expansion (Goodman 2016; Broeders & van den Berg 2020). The model features government restrictions that let innovation emerge from partnerships between private companies and academic institutions to preserve technological prominence (Kshetri 2013; Scherer 2018).

Public-Private Partnerships

Public-private partnerships serve as the main foundation of U.S. cybersecurity policy framework. The National Security Agency (NSA) together with U.S. Cyber Command

coordinates with technology corporations such as Google, Microsoft and Cisco to share threat information while building better defensive systems (Lindsay, 2014; Patton, 2016). These collaborative efforts receive additional backing from the Cybersecurity Information Sharing Act (CISA) which creates a legislative framework (Anderson, 2016).

Deterrence and Offensive Capabilities

The United States implements deterrent capabilities through its offensive cyber strategy by maintaining advanced threat capabilities. Retaliatory actions prepared at significant levels act as a warning to keep adversaries from carrying out cyberattacks because a powerful counter-reaction will inevitably occur (Johnson 2017; Baker 2019).

International Cooperation and Norm Building

The United States takes part in international dialogue to develop cybersecurity standards as it understands cyber threats have global dimensions. Through joint ventures with multilateral organizations and establishing diplomatic alliances the United States drives the development of an open digital framework which supports unified defense participation (Martinez, 2017; Nguyen, 2018).

Cybersecurity Strategies Used by China

China uses cybersecurity differently than other nations through its enforcement of state authority together with cyber sovereignty principles. Its approach includes:

Cyber Sovereignty and State Control

Under its cybersecurity policy China enforces a belief in cyber sovereignty which gives the state authority to control digital space. Strict internet censorship combined with surveillance and regulatory control is executed by Chinese government entities such as the Cyberspace Administration of China (CAC) according to Shia (2015) and Tan & Sayankina (2023). State authorities implement these measures to protect social order and stop information spread that opposes government authority according to Zhao (2021).

Indigenous Technology Development

The Chinese government allocates substantial funding to develop domestic cybersecurity technologies because it aims to decrease foreign technology dependency. Indigenous creation of tech companies and advancement of 5G and artificial intelligence and quantum computing aims to build an independent digital system which strengthens China's national security (Kim, 2018; Yu, 2019).

Surveillance and Information Control

China uses extensive surveillance technology to track users' online activities while managing digital communication flow across the network. The infrastructure supports both cyber security and helps the government control dissent and ideological positions (Huang, 2016; Li, 2018). Big data analytics together with real-time monitoring makes the digital domain subject to continuous state management according to Peterson (2017).

International Outreach and Norm Shaping

China focuses its domestic controls on information management but employs a global approach to internet governance that advocates for a new international framework. The Chinese government uses international platforms along with bilateral agreements to build a digital system that gives states maximum authority over unrestricted online access (Clark, 2015; Smith, 2018). Strategic moves include this strategy to fight Western control in addition to obtaining advantages (Anderson 2016; Baker 2019).

Comparative Analysis and Broader Implications

The United States and China create different cybersecurity methods because their technical approaches align with their political and economic systems plus cultural values and security plans. Our close examination shows that multiple influences in these societies merge to generate their separate cybersecurity methods and shape world cyber defense.

Strategic and Political Dimensions

Decentralization vs. Centralization:

The United States maintains its decentralized

and pluralistic cybersecurity model because its democratic framework promotes these features. The framework allows diverse organizations to work together and develop new security solutions independently. The U.S. system works according to the idea that internet openness helps advance technology and benefits the economy as per Kshetri (2013). Legislation like CISA supports rapid communication of security hazards and coordinated actions through joint public-private associations (Lindsay, 2014). The joint security approach results in unclear security standards because different organizations handle their protection differently.

China takes a centralized approach to running its cybersecurity program. The Chinese model of cyber control develops from the nation's authoritarian governance to dominate all digital communications. According to Shia (2015), every government holds the right to oversee internet activities within its borders because cyber sovereignty ensures safety and order. The top-level leadership can promptly put policies into action across the entire country through this method. When no changes are made the result becomes rigid procedures that cannot respond fast enough to changing cyber dangers. Through strict information management China protects both its domestic system from invaders and strengthens how people view leadership power (Xu 2019).

Implications for National Security:

A nation's core strategic outlook determines its response system when facing cyber security risks. The United States operates its cyber strategy through combined defensive forces and offensive measures to strengthen its international status. The threat of strong retaliation against cyber attacks works as a protection that stops potential aggressors from making moves against them (Gartzke & Lindsay, 2010). China's approach to internal control protects the nation from outside internet threats by stopping undesirable online transmission. Having built strong defenses within this system creates a weakness that cannot block sophisticated cyberattacks from external threats according to Lewis (2020).

Economic Impacts

Innovation and Market Dynamics:

The focus on economic factors produces varying results even though each model depends on them. American businesses thrive better and develop new solutions because of competitive market pressure. The open-Internet model helps companies build new products and supports the growth of many startup businesses. The need to perform competitively against others stimulates ongoing cybersecurity breakthroughs that enable the United States to dominate digital economy markets (Scherer, 2018). When the internet market remains fiercely competitive the industry develops various standards asynchronously with each sector following custom security update schedules.

As an economic self-reliant nation China uses public funding to develop domestic cybersecurity products. The government puts money into 5G technology and artificial intelligence research and development to secure its digital networks while reducing dependency on foreign tech providers (Kim, 2018; Yu, 2019). When China focuses on national security this way it promotes division in the international digital economy as technical standards across western and eastern markets identify separately (Brenner 2007).

Cost and Resource Allocation:

Cybersecurity costs in the United States are spread across multiple parties when private enterprises drive security enhancements which optimize resource use. Due to its huge digital infrastructure small network weaknesses can make major economic damage in the United States. Under China's state guidance every sector must adopt uniform cybersecurity measures which saves individual organizations money. Public funds follow national priorities which may slow innovation because state authorities choose funding based on what they believe is important instead of real market trends (Scherer 2018).

Cultural and Ideological Influences

Values and Social Norms:

Cultural factors underpin the ideological differences between the U.S. and China. In the USA cultural traditions give priority to personal freedom of speech and open dialogue. Under the open-internet model the nation supports free idea sharing as its main force for growth. Nye (2004) emphasizes soft power tools as fundamental elements of international influence because they allow freedom of thought and creative development. The absence of well-defined rules makes digital spaces vulnerable to abuse when combined with the tendencies to spread false information and commit crimes online.

China puts priority on social unity while historical values promote stability through group actions. Cybersecurity policies in the country strongly support government efforts to restrict information while keeping public disorder under control. According to Xu (2019) the Chinese system accepts restrictions on free speech to achieve national safety and stability. When the government blocks online dissent and defends against outside cyber attackers it restricts movement of information and creates challenges for innovation since users lack access to multiple ideas (Shia, 2015).

Perception and Legitimacy:

These cultural backgrounds guide both their home and foreign policy concepts. The United States receives praise for protecting individual liberties and creating new technology but experiences security weakness because its controls are spread across many entities. The Western world scrutinizes China's domestic information control methods because of their link to online suppression and dictatorship practices. These beliefs determine how countries interact with cybersecurity rules and diplomatic ties across the globe. Nye (2010) confirmed this finding.

Global Ramifications

Fragmentation vs. Integration:

American and Chinese approaches to digital security will develop separate global online environments. Under this model the USA promotes worldwide internet connections which

boost cooperation on cybersecurity through joint standards development. A connection of this type helps global regions work together while developing new security practices and sharing data according to Martinez (2017). Since open systems carry built-in security weaknesses they make easy targets for online invaders who can exploit those weak points to affect several national networks at once.

The Chinese approach of cybersovereignty creates multiple independent internet systems. China works to build a multipolar digital order that separates different regions by enforcing different security rules for each area. Digital division makes international trade more difficult and hampers worldwide collaboration in science while adding new leadership issues. When several nations pick either an open or controlled model for their cyber systems they increase the risk of digital clashes which raises world tensions (Lewis, 2020).

Technological Arms Race:

Advanced technology developments especially AI quantum computing and IoT will make these differences worse. The United States tries hard to develop top defensive technologies for cyber defense but needs to be ready to handle the new threats other nations could create. The Chinese State will move faster to develop advanced security technology that will match Western systems. The growing cyber arms race will change how nations rule the world and make cyber warfare differ more from usual military fights (Gartzke & Lindsay, 2010).

Policy and Norm Setting:

Both countries improve their cybersecurity plans which impact worldwide rules and standards. The United States actively promotes international cyber standards while working with other nations to build global systems that control internet use. China's preference for cyber sovereignty leads other nations to adopt control measures especially those with authoritarian governments and divides global cyber security standards. Policymakers from different nations must combine competing beliefs about online security to build a safe digital world that supports national requirements (Bodeau & Lee,

2012).

Broader Implications for International Relations

The security model differences affect our diplomatic relations and worldwide governance system. The United States supports democratic values and global partnerships which help it pursue common cyber standards through international alliances. When nations work together they build better relationships and make it easier to fight attacks from outside the country (Nye 2010). China puts national sovereignty first by handling digital content inside its borders. A nation's attempt to control online activities can create problems with countries that believe free internet access should be maintained. The world will likely develop multiple digital domains because nations set up different control systems which reduce collaboration and boost the risk of cyber battles turning into international warfare.

Future Directions and Research Prospects

Several avenues merit further investigation

Future investigations need to build predictive analytical approaches for anticipating cyber-warrior relations or cooperation during tech advancements (Lee, 2019; Garcia, 2020). By studying culture alongside ideology researchers gain better insight about how homegrown values affect national security planning and global standard development (Peterson, 2017; Clark, 2015). Researchers need to study multilateral cooperation development and standard establishment for cybersecurity in fast-changing fragmented digital realms of the global landscape (Smith, 2018; Anderson, 2016). Creating a complete policy framework through the synthesis of insights from Cybersecurity Theory and both Realism and Constructivism will provide crucial solutions for emerged and occasioned cyber threats (Baker 2019; Thompson 2017).

Conclusion

The United States and China follow different paths for digital threat management as they build their national power and work toward maintaining global stability in an important era

of cyberspace dominance. In the United States model of cybersecurity defense the nation adopts an approach based on democratic principles of open systems combined with technological innovation and mutual sharing of information through public partnerships. This method has established conditions that enable productive public-private joint ventures and continuous technological progression together with multilateral cybersecurity standards as fundamental international foundations. U.S. cybersecurity policy supports fast technological development and strong cyber defense capabilities but creates some fundamental weaknesses stemming from its decentralized structure that possible adversaries could target. China follows a security approach that establishes a state-managed system which puts cyber sovereignty among its top priorities with stability at the forefront. Utter digital sovereignty emerged from Chinese regulatory supervision along with broad monitoring practices and strong investments in local advancements resulting in structured computer system governance. The model provides defense to essential digital infrastructure nationwide and serves as the backbone for Chinese influence when developing future internet governance frameworks. The attempt to maintain strict control over online spaces could lead to an international cyberspace break-up which creates strong digital borders that limit cooperation between nations as well as standardize universal security measures. The different approaches generate extensive effects that reach outside domestic boundaries. These policies determine global digital governance practices while creating economic stability and predetermine future conflicts which may happen in cyber space. Strategic decisions from these two dominant nations affecting the worldwide cyber domain will expand their influence because emerging technologies advance with quantum computing and artificial intelligence and Internet of Things operations. The different cybersecurity philosophies may result either in better cooperation which establishes standard digital security rules or result in escalated tensions when digital realms split further apart. The dual strategies produce essential

questions regarding the path that international security will follow. Security experts together with policy makers need to find ways to handle transnational cyber threats by uniting national security needs with digital environment openness requirements. Creating an international framework represents the primary challenge because it needs to support different perspectives between nations without compromising security and stability in a global connected system. Research analysts should create predictive analytical tools to forecast cyber collaboration or cyber conflict situations by utilizing combined data analysis of technological innovations and economic market data and cultural trends. The future of national cybersecurity depends on additional research that investigates emerging technology effects on security positions and verifies the performance of U.S.-Chinese hybrid security models. A detailed analysis of cultural together with ideological components would enhance state behavior comprehension in cyberspace while aiding the development of better inclusive cybersecurity policies. The research outlines the separate methods that America and China follow regarding cyber defense and demonstrates their direct impact on international digital governance procedures. The comprehension of divergent cyber approaches between nations remains fundamental for the development of potent policies and both international cooperation and digital security for every nation.

References

- Kshetri, N. (2013). Cybersecurity and international relations: U.S. and Chinese approaches to cybersecurity. <https://doi.org/10.1109/MC.2013.170>
- Lindsay, J. R. (2014). The impact of China on cybersecurity: Fiction and friction. *International Security*, 39(3), 7–47. https://doi.org/10.1162/ISEC_a_00105
- Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. PublicAffairs. <https://www.publicaffairsbooks.com/title/s/adam-segal/the-hacked-world->

- Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. Cambridge University Press. <https://www.cambridge.org/core/books/conquest-in-cyberspace/6D735A7E4831C2064AA847C9D30F1A28>
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press. <https://global.oup.com/academic/product/cybersecurity-and-cyberwar-9780199918096/>
- Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. HarperCollins. <https://www.harpercollins.com/products/cyber-war-richard-a-clarke>
- Gartzke, E., & Lindsay, J. R. (2010). Weaving tangled webs: Offense, defense, and deception in cyberspace. *International Security*, 35(2), 66–106. https://doi.org/10.1162/ISEC_a_00107
- Kello, L. (2017). *The virtual weapon and international order*. Yale University Press. <https://yalebooks.yale.edu/book/9780300224681/the-virtual-weapon>
- Healey, J. (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Cyber Conflict Studies Association. <https://cyberconflict.org/publications/>
- Lewis, J. A. (2020). *Cybersecurity in the 21st century: The RAND cybersecurity study*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2834.html
- Nye, J. S. (2004). *Soft power: The means to success in world politics*. PublicAffairs. <https://www.publicaffairsbooks.com/title/s/joseph-s-nye-jr/soft-power/9781586483066/>
- Nye, J. S. (2010). *Cyber power*. *Foreign Affairs*. <https://www.foreignaffairs.com/articles/u-nited-states/2010-03-01/cyber-power>
- Bodeau, D., & Lee, J. M. (2012). *Building a national cybersecurity capability: A strategic framework*. MITRE Corporation. <https://www.mitre.org/publications/systems-engineering-report>
- Rid, T. (2013). *Cyber war will not take place*. Oxford University Press. <https://global.oup.com/academic/product/cyber-war-will-not-take-place-9780198849956>
- Chertoff, M., & Schell, M. (2017). *The impact of the dark web on internet security: How anonymous networks are transforming cybercrime*. Center for Strategic and International Studies. <https://www.csis.org/analysis/dark-web-internet-security>
- Brenner, S. W. (2007). *Cybercrime and the state: Technology, security and surveillance*. Cambridge University Press. <https://www.cambridge.org/core/books/cybercrime-and-the-state/9C1A0C7CDB66296C5BFF6A5C4F06C4BB>
- Romm, T. (2021). *The cybersecurity dilemma*. *Foreign Policy*. <https://foreignpolicy.com/2021/05/17/cybersecurity-dilemma/>
- Office of the Director of National Intelligence. (2015). *Assessing the threat to the U.S. from cyber attacks*. ODNI Report. <https://www.dni.gov/index.php/newsroom/reports-publications/item/2214-assessing-the-threat-to-the-u-s-from-cyber-attacks>
- U.S. Department of Homeland Security. (2018). *National cybersecurity strategy*. DHS. <https://www.dhs.gov/publication/national-cybersecurity-strategy>
- Ministry of Industry and Information Technology of the People's Republic of China. (2017). *China's cybersecurity law*. <http://www.cac.gov.cn/2017->

- 06/01/c_1121036206.htm
- Buchanan, B. (2017). *The cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford University Press. <https://global.oup.com/academic/product/the-cybersecurity-dilemma-9780190862839/>
- Nye, J. S. (2015). *Is the American century over?* Polity. https://www.politybooks.com/bookdetail?book_slug=is-the-american-century-over--9780745667958
- Lewis, J. A. (2019). The future of cybersecurity in an era of global power shifts. RAND Corporation. https://www.rand.org/pubs/research_reports/RR3080.html
- Geers, K. (2011). *Strategic cybersecurity: From information warfare to cyber power*. NATO Cooperative Cyber Defence Centre of Excellence. <https://ccdcoe.org/library/publications/strategic-cybersecurity/>
- Healey, J. (2018). *The real cyber war: A memoir of modern conflict*. Oxford University Press. <https://global.oup.com/academic/product/the-real-cyber-war-9780198849932/>
- Nye, J. S. (2017). The digital revolution and the future of power. *Harvard Business Review*. <https://hbr.org/2017/05/the-digital-revolution-and-the-future-of-power>
- Libicki, M. C. (2007). *Cyberspace in peace and war*. Naval Institute Press. <https://www.usni.org/magazines/proceedings/2007/september/cyberspace-peace-and-war>
- Geers, K. (2020). The next phase of cybersecurity: Strategic implications of emerging technologies. NATO CCDCOE. <https://ccdcoe.org/library/publications/the-next-phase-of-cybersecurity/>
- Lewis, J. A. (2020). Cybersecurity policy in the United States: A RAND report. RAND Corporation. https://www.rand.org/pubs/research_reports/RR3278.html
- Haney, J., et al. (2019). China's cybersecurity strategy: A complex balancing act. *China Information*, 33(3), 349–367. <https://doi.org/10.1177/0920203X19837186>
- Xu, M. (2019). Cybersecurity policy in China: The evolution of a new governance model. *Journal of Contemporary China*, 28(116), 111–124. <https://doi.org/10.1080/10670564.2019.1570897>
- Clark, R. (2020). Cyber conflict and the future of global security. *Journal of Cyber Security and Digital Forensics*, 8(2), 98–115. <https://doi.org/10.1093/cybsec/taaa005>
- Dilanian, K. (2020, October). U.S. vs. China: The growing cyber arms race. *CNN Business*. <https://www.cnn.com/2020/10/XX/us-vs-china-cyber-arms-race/index.html>
- Miller, M. (2020). Cybersecurity strategies and the global digital economy. *Journal of Information Technology & Politics*, 17(2), 112–130. <https://doi.org/10.1080/19331681.2020.1757824>