China’s Authoritarian Grip
How China Reinforces Social Control, Cultivates a Climate of Fear, and Minimizes Dissent
LCDR JORDAN J. FOLEY, JAGC, US NAVY

Abstract
Roughly one-quarter of the world’s people and Internet users live under governments that engage in heavy censorship. A large portion live behind “The Great Firewall” of China, which places strategic importance on Internet control. The Internet can serve counterhegemonic purposes, as numerous groups in civil society use it to connect isolated populations, unite women’s movements, and enable human rights and political minority activists. However, China sees Internet censorship as crucial for national security and social stability. Through legal research, translating Chinese sources, and drawing on personal experiences in China, this paper argues that Chinese domestic censorship poses an international threat.

***

In 2012, I completed a Personnel Exchange Program (PEP) with the People’s Liberation Army Navy (PLAN) at the Lüshun Naval Base in Dalian, China. My experience serving alongside both PLA soldiers and sailors has informed many of my views about the People’s Republic of China’s (PRC) military build-up and increasingly aggressive behavior toward US military operations. During this PEP, we completed naval drills, military training, and team-building exercises. For one exercise, I was on a team with four British and Australian naval officers for a 10-kilometer (km) “ruck run.” Our team took off and ran the 10-km course as designed, weaving through the hills and coastline of the Bohai Straits. The rules were: (1) follow the path and (2) do not lessen your weight. After the 10-km, we approached the finish line only to find the PLA team had finished and won without us ever seeing them pass. After a brief confrontation, it was revealed that the PLA members had dropped much of their weight and took a shortcut, essentially halving the course to 5 km. When I called out one of the PLA officers, rather than admitting they cheated or denying more furiously, he simply said, “You could have done that too and you didn’t. You lost.” That reaction and statement to what I considered blatant cheating should be an important lesson not just for bravado competitions like a ruck run, but it should inform how the United States and its allies and partners approach the PRC in the coming decades. From the Chinese mindset, it is not cheating—it is competing.
Chinese conceptions of the rules-based international order are not aligned with a free and open world. This disregard for individual freedoms is most pronounced in China’s domestic Internet-control mechanisms. “The Great Firewall” system began in 2006 and now extends beyond the Internet to include digital identification cards with microchips containing personal data that allow the Chinese Communist Party (CCP) to recognize faces and voices of its 1.3 billion-plus inhabitants. China’s government-led program of Internet development serves as a model for other authoritarian states elsewhere. The Great Firewall is the envy of authoritarian regimes worldwide, and versions have been exported to Cuba, Iran, and Belarus.¹

The reluctance of some Western countries to stand up for ideals that have done so much to achieve human rights and correct the hardships of an imperfect world could be caused by China’s economic and political power.² However, the desire to stand up to China is growing and must be encouraged.³ In early 2020, India amended its foreign direct investment policy to enforce tougher scrutiny on Chinese investors. That same month, an Indian app developer created a top trending program called “Remove China Apps,” which was downloaded more than 5 million times. It enabled users to detect and easily delete apps developed by Chinese firms.⁴ The desire to promote a free and open Internet is prevalent in interest groups as well. For example, the Falun Gong religious movement, using programmers in the United States, developed censorship-circumventing software called “Freegate,” which it offered to dissidents elsewhere, particularly in Iran.⁵

The relationship between Chinese censorship and free Internet advocates forms a continual change of strategies and tactics. As one Chinese netizen put it, “It is like a water flow—if you block one direction, it flows to other directions, or overflows.”⁶ As the Internet increasingly becomes an arena of conflict, much like the open seas, the United States must show that freedom of navigation on the web is for all humankind.⁷ The world’s democracies must, as President Ronald Reagan

---

⁵ Warf, “Geographies of Global Internet Censorship.”
⁶ Warf, “Geographies of Global Internet Censorship.”
⁷ Andrew Kassoy, Bart Houlahan, and Jay Coen Gilbert, “Impact Governance and Management: Fulfilling the Promise of Capitalism to Achieve a Shared and Durable Prosperity,” Brookings Institute, 1 July 2016, https://www.brookings.edu/.
China’s Authoritarian Grip

said, “be worthy of freedom and determined not only to remain so but to help others gain their freedom as well.”

The Great Firewall

The CCP’s mandate to govern 1.35 billion people is founded on its promise to restore the country to a prime position in the regional and global order. The CCP cannot do that without control of the Internet. China’s concept of Internet sovereignty is a belief in each country’s right to stop unwanted information at its borders. This is a fundamental tenant of CCP social control. Beijing expends resources and manpower on a massive scale to ensure content censorship and preventing dissemination of “moral pollution.” China, with nearly 700 million users operating behind The Great Firewall, is strangling its Internet in its desire to maintain political and social control.

The CCP has a vested interest in the continuous development of information warfare (IW) capabilities directed at domestic content. State-run news media outlets actively seek to influence Western perceptions, while the CCP contends that Western media outlets not only exhibit bias but also participate in a coordinated international effort to tarnish China’s reputation. If a free and open Internet is increasingly recognized as a human right, then the Chinese Internet, intentionally designed to suppress its people, unequivocally violates this principle. Far from serving as a platform for the free exchange of ideas, China’s Internet reinforces social control, fosters a climate of fear, and suppresses dissent. While China’s initial justification for imposing censorship was rooted in concerns over public morality, particularly regarding issues like pornography and gambling, in recent times, the primary rationale has shifted toward combating terrorism.

These deliberately vague notions of national security have contributed to the ongoing situation in Xinjiang, China’s western province predominantly inhabited by ethnic Uighur Muslims.

8 Gallagher, “The Lost Art of Ideological Warfare.”
12 Xu and Albert, “Media Censorship in China.”
A comprehensive understanding of the history of the Internet in China is essential. Equally vital is an appreciation of the CCP’s intricate relationship with the Internet. Unlike democratic nations, the Chinese Internet exists in relative isolation from the rest of the world. Since its introduction in 1994, the CCP’s paramount concern has been the potential political instability that the Internet could precipitate. In 2000, to exert control over information accessibility, the Party initiated a surveillance system capable of accessing the digital records of every citizen. This project primarily focused on individual user surveillance and later became known as “The Great Firewall.” Its success hinged on three primary methods: Internet Protocol (IP) blocking, IP address misdirection, and data filtering. Importantly, every action undertaken by the CCP to control the Internet is deemed legal within the framework of Chinese domestic law.

The effectiveness of “The Great Firewall” does not solely stem from its technological prowess but also from the culture of self-censorship pervasive in China. Chinese companies bear responsibility for the content hosted on their websites and are held liable if they fail to report and remove content conflicting with the CCP’s narrative. These companies are required to engage in self-regulation characterized by a commitment to “patriotic observance of law, equitableness, trustworthiness and honesty.”

Even US corporations are opting for self-censorship to safeguard the substantial profits derived from their engagements with China. In July 2020, Apple made the decision to remove thousands of games from its Chinese App Store in response to a policy mandating that all paid games or games featuring in-app purchases must be licensed by Chinese regulators. Apple provided no specific guidance to app developers regarding content that contravened Chinese regulations; instead, there was an abrupt and sweeping removal. Amid this purge, Apple also withdrew the popular iOS and Android podcast client, Pocket Casts, from the Chinese App Store. The Cyberspace Administration of China determined that Pocket Casts

---

14 Warf, “Geographies of Global Internet Censorship.”
China's Authoritarian Grip

could potentially provide access to content considered illegal within the country and thus demanded its removal. This marked the second prominent podcast app removal from China's App Store.

Impacts on US Tech Companies

Even previously exploited loopholes by banned game developers are being closed not by the CCP but by the US platforms through which these games are distributed. Profit-driven enterprises, such as Rockstar Games, had previously relied on these loopholes to sell titles from the Grand Theft Auto franchise within the nation. However, in February 2020, Apple initiated reminders to developers that obtaining licenses was a requisite, lest their games face prohibition and removal. Android app stores have similarly enforced this licensing prerequisite for publication.20

Public platforms bear ultimate responsibility for the content they host.21 The Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry mandates that Chinese tech companies actively monitor their websites and eliminate any prohibited material. Chinese Cybersecurity Law governs publicly accessible information and is legitimized by the Chinese legal doctrine of cyberspace sovereignty.22

In the international arena, the principle of sovereignty may appear incongruent with cyberspace. Traditionally, violations of sovereignty pertain to physical acts within the territory of other states. Sovereignty is a concrete, territorial concept, while cyberspace establishes connections between states that seem ethereal in nature. Yet, these two concepts coexist. States and the international community are striving to harmonize the ideals of an unimpeded flow of information in cyberspace with a state’s authoritative control over cyber activities within its borders.23

An increasing number of states, such as China, staunchly advocate for sovereignty over an open and unrestricted cyberspace. For liberal democracies, countering this trend is of paramount importance.

Sovereignty violations can be grounded in two distinct criteria: “(1) the degree of infringement upon the target state’s territorial integrity; and (2) whether there

---

has been an interference with or usurpation of inherently governmental functions.”\textsuperscript{24} The Tallinn Manual 2.0 working group has argued that remote cyberoperations leading to tangible consequences, such as the replacement of hard drives, qualify as such violations. However, the classification becomes less clear when misinformation directed into another state’s borders triggers a physical response, such as rioting and looting.

**Censorship and Gaming Companies**

Article 12 of China’s Cybersecurity Law serves as the basis for addressing violations where technology is used to “incite subversion of national security . . . [or] disseminate violent, obscene, or sexual information.”\textsuperscript{25} Consequences for such violations may range from the removal of an application to heightened content regulation or temporary bans on specific characters or gameplay within China. Notably, China’s cybersecurity regulations place a significant focus on technology companies referred to as network operators.\textsuperscript{26} The Cybersecurity Law specifically defines network operators as “network owners, managers, and Internet service providers.”\textsuperscript{27}

For network operators operating within industries deemed “critical infrastructure,” additional regulations come into play.\textsuperscript{28} Article 21 of the Cybersecurity Law mandates that these network operators must adhere to a tiered cybersecurity protection system. To engage in business within China, companies must implement technical measures for monitoring and recording network activities, as well as providing technical support for Chinese investigations.\textsuperscript{29} Companies within this designation must also store personal information and other “important data” within the borders of the PRC. The term important data refers to data, as determined by the CCP, closely linked to national security, economic development, and public interest. Leaking or misuse of such data after it is transferred outside of China can have severe consequences. Companies classified as network operators handling


\textsuperscript{26} Punyakumpol, “The Great Firewall of China.”

\textsuperscript{27} “Translation: Cybersecurity Law,” art. 76.

\textsuperscript{28} “Translation: Cybersecurity Law,” art. 21.

important data under the Cybersecurity Law face heightened scrutiny, placing them in a category subject to the most rigorous oversight. Even Chinese network operators in noncritical industries must secure prior consent from individuals when transferring data across borders. Furthermore, they must demonstrate that such data export is essential for routine business operations or contractual obligations. Additionally, these data exports must align with relevant treaties and pass a security assessment conducted by the network operator. The mandatory security assessment evaluates the suitability and risk management of the data export plans. If the assessment yields a high-risk outcome, personal information and important data cannot be exported, and the results of the assessment must be retained and reported.

**Cybersecurity Law and Data Localization**

Territorial integrity and inviolability stand as bedrock principles in international law. For cyberespionage conducted within another state’s borders to be considered lawful, it would necessitate a customary exception to the general principle of territorial integrity and inviolability. Given that the potential political fallout may outweigh the benefits gained from such operations, sovereignty-violating cyber campaigns might only be pursued as a last-resort measure, with a full understanding of the potential reactions they may trigger.

China’s perspective on cyber sovereignty encompasses both the technology and the actual data transmitted and stored across the Internet. China views ownership over data and information networks as a key to ensuring both a secure Internet and national security. This perspective is exemplified by President Xi Jinping’s statement that “without cybersecurity, there is no national security.” Consequently, China’s approach to cyber governance is closely tied to national security concerns. The Chinese National Security Law, enacted in July 2015, grants the CCP substantial authority to implement a robust cybersecurity framework.

---

30 “Translation: Cybersecurity Law,” art. 16.
Although it may appear that the Internet transcends borders, it is not entirely borderless; traditional concepts of sovereignty remain applicable cybersovereignty. China’s Great Firewall serves as a regulatory mechanism governing the country’s domestic network and cyber infrastructure to enforce its concept of cybersovereignty. In this view, state boundaries delineate not only the confines of the state’s corresponding cyberspace but also any internal effects of cyberoperations are perceived as a challenge to sovereignty by the CCP.\textsuperscript{35} The CCP regards a free and open Internet as a threat to China’s sovereignty.\textsuperscript{36}

Online privacy protection in China remains a complex landscape, comprised of a myriad of laws, regulations, and judicial interpretations.\textsuperscript{37} A significant milestone occurred with the enactment of the Cybersecurity Law in 2016, marking the first direct legal protection of “personal information.”\textsuperscript{38} This legislation lays out precise requirements for entities involved in the collection, retention, and processing of such information. An especially critical mandate, particularly for international corporations operating within China, pertains to data localization.\textsuperscript{39} Nations asserting strong cybersecurity sovereignty, such as China and Russia, often mandate that data gathered within their borders must be stored within the country. Data localization grants China enhanced control over online content through its jurisdictional authority over the stored data.

**US Law and Actions in Cyberspace**

The Department of Defense (DOD) defines cyberspace as a global domain within the information environment that comprises the interdependent network of information technology infrastructures and resident data. This includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.\textsuperscript{40} In September 2018, the White House released a national cyber strategy consisting of four pillars, one of which aimed to promote the extension of the key principles of an “open, interoperable, reliable, and secure internet.” When


\textsuperscript{36} “Translation: Cybersecurity Law,” art.1.


applied to China, implementing any measures to enhance Internet transparency necessitates an examination of covert action operational law.

This general sense of “covert” aligns closely with, but is slightly broader than, the US statutory definition of *covert action*. According to the National Security Act, *covert action* refers to activities undertaken by the US government (USG) to influence political, economic, or military conditions abroad. The intention is that the role of the USG will not be publicly apparent or acknowledged. However, this excludes certain categories of government conduct, such as intelligence gathering and traditional diplomatic, military, or law enforcement activities.41

Entering China’s cyberspace domain requires a comprehensive legal and ethical analysis. Strategists must also evaluate US domestic, international, and Chinese laws to determine if an action violates any legal principles. If it is found to be contrary to established laws, the United States must then consider whether these challenges can be overcome or if such operations are illegal. Understanding the “facts on the ground” serves as the initial step, but a US cyber operation aimed at identifying vulnerabilities in The Great Firewall of China finds its legal basis in the US Covert Action statute.

The rationale behind categorizing this operation as a *covert action* is that it provides the most suitable legal framework and operational flexibility to achieve the stated policy objective. Under Title 50, U.S. Code, War and National Defense, Section 3093 (‘50 U.S.C. 3093’), a covert action requires a presidential finding and notification to the Intelligence Committee. This section enables the president to authorize a covert action if it is deemed necessary to support identifiable foreign policy objectives of the United States and is crucial for national security.

The FY2018 National Defense Authorization Act (NDAA) mandated notification of the use of cyberweapons and quarterly cyberoperations briefings to the Congressional Armed Services Committees. Although the Obama administration’s classified Presidential Policy Directive 20 (PPD-20) governed US cyberoperations policy, it did not grant new authorities. According to former officials, PPD-20 mandated interagency approval for significant cyberoperations. In September 2018, the White House acknowledged its replacement with new guidance, the National Security Presidential Memorandum 13 (NSPM-13), which grants greater authority to the commander of US Cyber Command (USCYBERCOM).42

---


authority structure authorizes covert actions to secure US interests by conducting military and foreign intelligence operations in cyberspace.

The president has the authority to designate which department, agency, or entity of the USG will participate in the covert action. The sponsorship of a covert action is hidden, not the act itself. Whereas for clandestine acts, the act itself—for example, intercepting a phone call—must remain concealed. Additional levels of secrecy can also hinder effective policy implementation, sometimes with dramatic national security consequences.

When nonconsensual cyberoperations below the threshold of a prohibited intervention violate international law, it is a question that must be resolved through the practice and opinio juris of states. It must develop over time and in response to the needs of states to effectively defend themselves and provide security for their citizens. Meeting international legal standards in this context may present challenges.

International Law and Cybersovereignty

States are increasingly employing cyberspace as a new avenue for traditional statecraft at a rapid pace. Activities that bolster national security, such as espionage, and low-cost, asymmetric offensive operations, can now be exclusively executed within cyberspace. International law, through both custom and treaties, establishes clear prohibitions against unlawful uses of force and intervenes in certain state-to-state interactions.

The law of war governs the conduct of armed hostilities, encompassing all international laws that bind the United States, including treaties, international agreements to which the United States is a party, and applicable customary international law. Furthermore, DOD policy extends the fundamental principles of the law of war to cyberspace operations. International law neither inherently forbids covert conduct nor exempts it from legal scrutiny. However, a covert action in cyberspace may potentially violate international law, including principles related

---

44 Perina, “Black Holes and Open Secrets.”
46 Egan, “International Law and Stability in Cyberspace.”
47 Egan, “International Law and Stability in Cyberspace.”
to sovereignty and noninterference.\textsuperscript{48} Notably, sovereignty alone does not preclude cyber activities when they remain below the threshold of intervention.

The challenges of disentangling the political, legal, and moral aspects of covert actions in cyberspace are formidable. Firstly, the lawfulness of state conduct under international law does not depend on the internal and often unknowable political motives.\textsuperscript{49} In other words, a political motive, such as preventing atrocities, does not absolve an act if it is inherently unlawful. Secondly, it remains unclear whether a nonconsensual cyberoperation falls below the threshold of prohibited intervention or breaches international law. The lawfulness of covert actions in cyberspace varies depending on interpretation, as observed through an examination of US domestic, international, and Chinese law. Thirdly, sovereignty alone might not prevent cyberoperations, and the criteria for unlawful intervention or use of force are stringent. Nevertheless, sovereignty remains an unresolved issue in cyberspace.

Perhaps the most operationally relevant legal issue within the cyberenvironment pertains to identifying criteria for determining when cyberoperations directed against a state violate its sovereignty. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (“Tallinn Manual”) addresses this issue, asserting that a “State must not conduct cyber operations that violate the sovereignty of another State.” This rule represents a significant red line between lawful and internationally wrongful conduct based on “(1) the degree of infringement upon the target state’s territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions.”\textsuperscript{50} The Tallinn Manual cites the Island of Palmas arbitral award, which sets forth the authoritative crux of sovereignty, holding, “[s]overeignty in the relations between states signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.”\textsuperscript{51} This categorization includes some actions that are coercive, such as acts manipulating the choice of a political, economic, social, and cultural system, as well as the formulation of foreign policy.\textsuperscript{52}

While the nonintervention rule is firmly established in customary international law, there exists limited state practice or \textit{opinio juris} on its applicability to cyber activities. An illustrative example of a violation of the principle of nonintervention


\textsuperscript{50} Schmitt and Vihul, \textit{Tallinn Manual 2.0}, Rule 4, “Violation of Sovereignty.”


\textsuperscript{52} Nicaragua v. United States of America.
through cyber activities occurs when State A coercively interferes in the internal political process of State B by digitally altering the recorded votes, affecting State B’s election results. Determining whether a nonconsensual cyberoperation falls below the threshold of prohibited intervention or constitutes a violation of international law is a matter that requires resolution through the evolving practice of states, responding over time to the need to defend themselves and ensure security for their citizens.

Setting aside the issue of sovereignty, any disregard for another state’s territorial integrity and inviolability constitutes an internationally wrongful act. Activities such as aerial trespass, unconsented-to actions in the territorial sea and on land, the causation of radioactive pollution in national airspace, and the exercise of enforcement jurisdiction abroad all violate the territorial integrity and inviolability of another state. However, the bar for unlawful intervention or use of force remains high. For instance, activities like minesweeping operations in another state’s territorial sea and excavation of channels and the establishment of a military presence on a state’s territory constitute violations of sovereignty, but they do not necessarily constitute unlawful interventions or uses of force. Covert actions in cyberspace aimed at breaching The Great Firewall may potentially violate sovereignty and are likely to contravene the Chinese perspective. Nonetheless, sovereignty does not necessarily prohibit cyber activities when they remain below the threshold of nonintervention.

Certain states hesitate to categorically affirm sovereignty as a principle that unconditionally prohibits specific types of cyberoperations. While sovereignty primarily functions to safeguard territorial integrity and inviolability, even a stronger Chinese stance in favor of nonintervention might not be adequate to bar these cyber activities. The legality of such actions hinges on whether they are construed as interventions. While certain cyberoperations clearly constitute interventions, such as the aforementioned infiltration of electoral processes, it remains unclear whether providing open channels of communication would be universally

---

53 Egan, “International Law and Stability in Cyberspace.”
interpreted as an intervention, especially if the objective is to expose potential human rights violations.

**Conclusion**

The Chinese government operates the world’s most intrusive mass surveillance system, yet consistently denies the international community meaningful access to it. China views the Internet through the lens of national security and sovereignty, differing significantly from the Western model that envisions citizens’ privacy rights in opposition to, rather than derived from, government authority.\(^{56}\) Even several years after the implementation of the Chinese Cybersecurity Law, many of its implications remain uncertain, but the potential of a technologically empowered totalitarian regime raises concerns for the future.

If the United States fails to underscore the ideological dimension in its competition with China, it risks overlooking a critical lesson from President Reagan’s Cold War struggle against the Soviet Union.\(^{57}\) Internet censorship should be regarded as a facet of a multifaceted network of contested relationships in cyberspace. The Internet serves as an arena of conflict that can advance various counterhegemonic causes, including human rights advocacy and ethnic or political movements in opposition to governments. In contemporary society, the Internet connects once-isolated and invisible populations. A free Internet empowers women’s movements, amplifies the voices of human rights activists, and provides a platform for political minorities to promote their agendas.

It is essential to recognize that the Chinese people are not synonymous with the CCP. The populace can be influenced to support a free and open Internet in this ideological struggle. Clear strategic objectives must underpin effective policy. To paraphrase the war theorist Carl von Clausewitz, embarking on a conflict without a well-defined objective is folly. The United States must aim to deter strict domestic Internet controls, which all too often conceal persecution and ongoing atrocities. Atrocity prevention is a matter of national security, crucial for establishing democratic security and stability worldwide. In countries like Myanmar, where efforts are made to prosecute and silence minority populations, the United States should make it abundantly clear that the level of sophistication and resources required to prevent information leaks and international intervention renders such actions not worth the cost. Challenging China’s stranglehold on Internet freedom


\(^{57}\) Gallagher, “The Lost Art of Ideological Warfare.”
is a formidable task, as few other nations wield such comprehensive dominion over the web. However, unless the United States leads a multipronged effort to dismantle China’s grip on the freedoms of its people, we run the risk of authoritarianism spreading into other regions of the Indo-Pacific and beyond. 

LCDR Jordan J. Foley, JAGC, US Navy
Lieutenant Commander Foley is an active-duty naval officer serving as the Department Head for Maritime Law in the Office of the Navy Judge Advocate General at the Pentagon. Foley is a former submarine and space cadre officer and is an experienced national security operator. Foley has lived in China on three separate occasions, including one Navy-to-Navy exchange with the PLA Navy.

The views expressed in this article are those of the author and do not reflect the official policy or position of the firm or its clients, the Department of Defense (DOD), or the US government. The appearance of external hyperlinks does not constitute DOD endorsement of the linked website or information contained therein. The DOD does not exercise any editorial, security, or other control over the information you may find at these locations. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

Disclaimer
The views and opinions expressed or implied in JIPA are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Department of the Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government or their international equivalents.