Journal of Technology Law & Policy

Volume 28 | Issue 1 Article 1

January 2023

The People's War and Its Application to China's Legal Framework for Cybersecurity

Christopher J. Lin

THE PEOPLE'S WAR AND ITS APPLICATION TO CHINA'S LEGAL FRAMEWORK FOR CYBERSECURITY

Captain Christopher J. Lin[*]

Abstract

This Article addresses the growing threat of cyberattacks on critical infrastructure by examining China's response, particularly through its Cybersecurity Law (CSL), against the backdrop of global cybersecurity laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). The CSL, enacted in 2016, is analyzed within the context of Chinese military doctrine, specifically, the concept of the People's War introduced by Mao Zedong. Part I traces the historical evolution of the People's War, Part II explores its continued relevance in cyberspace, and Part III discusses how the People's War elements manifest in the CSL and related regulations. This Article argues that the CSL focuses on elevating China's defensive cyber capabilities across governmental and consumer sectors, diverging from the more consumer-privacy-centric approach of other global cybersecurity laws. Part IV delves into the challenges the United States faces in responding to the CSL and suggests potential paths forward to bridge strategic divides between the two countries in the realm of cyberspace. The introduction vividly portrays real-world scenarios of cyberattacks impacting critical infrastructure, setting the stage for the exploration of China's unique response in the subsequent sections.

* Judge Advocate, United States Army. Presently assigned as an LL.M. Candidate to Georgetown University Law Center. J.D., 2017, UCLA School of Law; B.A., 2013, University of California, San Diego. Member of the D.C. Bar. The author thanks Major D. Nicholas Allen, Brigade Judge Advocate, 1st Security Force Assistance Brigade, for his continuous support and encouragement, along with his insightful feedback and contributions. This Article is rooted in his infectious passion for scholarship and operational law. The views and opinions presented herein are those of the author and do not necessarily represent the views of the United States Government, the Department of Defense (DoD), or its components. Appearance of, or reference to, any commercial products or services does not constitute DoD endorsement of those products or services. The appearance of external hyperlinks does not constitute DoD endorsement of the linked websites, or the information, products, or services therein.

INTRODUCTION

A sudden power outage left a quarter-million residents without power or heat.[1] Telecommunication outages that rendered phone calls and data access impossible.[2] A control system failure that released raw sewage across public grounds.[3] Each scenario has occurred in the real world in the past two decades due to cyberattacks. In the United States, former Defense Secretary Leon Panetta voiced his concerns about a "cyber-Pearl Harbor" in which "aggressors can launch attacks with cyber-tools to gain control of our nation's critical infrastructure . . . causing physical destruction and loss of life on a scale that 'would paralyze and shock the nation.'"[4]

And China has observed and formulated a response to these concerns. On a cool Wednesday morning in the autumn of 2016, hundreds of attendees—including politicians and representatives from major technological companies—sat in plush white leather auditorium chairs, peering up at a video link projected behind a podium. Framed against a mahogany background and the striking red and gold colors of the Chinese

1. Sean Lyngaas, *Russian Military-Linked Hackers Target Ukrainian Power Company, Investigators Say*, CNN, Apr. 14, 2022, https://www.cnn.com/2022/04/12/politics/gru-russia-hackers-ukraine-power-grid/index.html [https://perma.cc/Y8KV-LRTV].

2. Kate Fazzini, *Power Outages, Bank Runs, Changed Financial Data: Here are the "Cyber 9/11" Scenarios that Really Worry the Experts*, CNBC (Nov. 18, 2018), https://www.cnbc.com/2018/11/18/cyber-911-scenarios-power-outages-bank-runs-changed-data.html [https://perma.cc/T4PA-V7BJ].

3. Tony Smith, *Hacker Jailed for Revenge Sewage Attacks*, REGISTER (Oct. 31, 2001), https://www.theregister.com/2001/10/31/hacker_jailed_for_revenge_sewage [https://perma.cc/85WS-HHYH].

4. Robert K. Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor*," 18 VA. J.L. & TECH. 289, 293–94 (2014).

flag, Xi Jinping, the general secretary of China, presented his opening remarks at the Wuzhen Summit, noting the importance of international cooperation in building a community in cyberspace while also ensuring inclusiveness and security.[5] His comments followed the National People's Congress's enactment of China's Cybersecurity Law (CSL) earlier that month, which would drive dialogue on the increasing awareness of cybersecurity and data rights, along with a rush by corporations to comply with the law.[6]

While the CSL was promulgated alongside a number of cyber-related laws across the globe in the past decade, including the General Data Protection Regulation (GDPR)[7] and the California Consumer Privacy Act (CCPA),[8] the CSL differs in that it places a distinct focus on elevating the country's defensive cyber capabilities across governmental and consumer sectors, as opposed to a more singular focus on consumer privacy. This Article argues that the CSL can be viewed within the framework of Chinese military doctrine—specifically, the CSL retains key elements of the People's War, a concept discussed by Mao Zedong, the founder of the People's Republic of China. Part I traces the evolution and legacy of the People's War from its origins in Mao's writings in the early 1900s to modern-day applications. Part II examines cyberspace as a new warfighting domain, with the People's War enjoying continued relevance. Part III discusses aspects of the People's War as they apply to the CSL and its surrounding regulations. Part IV explores the challenges that the United States faces in creating a balanced response to the CSL and a possible path forward in bridging the divide between the two countries' strategic approaches to cyberspace.

I. THE LEGACY OF THE PEOPLE'S WAR

Modern Chinese doctrine underwent numerous shifts within the past century, largely in response to external threats such as the Second Sino-Japanese War during World War II and observations of the Gulf War. These shifts can be broadly understood as three periods of differing focal points. Mobilization of the masses under the People's War was prominent

---

5. *Di San Jie Shijie Hulianwang Dahui* (*第三届世界互联网大会*) [*Third World Internet Conference*], YOUTUBE (Nov. 16, 2016), https://www.youtube.com/watch?v=cawjSOpXP-4 [https://perma.cc/577W-U62L].

6. *See, e.g.*, Huifeng He, *Cybersecurity Law Causing "Mass Concerns" Among Foreign Firms in China*, SCMP (Mar. 1, 2018), https://www.scmp.com/news/china/economy/article/2135338/cybersecurity-law-causing-mass-concerns-among-foreign-firms-china [https://perma.cc/N2WQ-CQPE].

7. *Data Protection in the EU*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [https://perma.cc/NU5F-P4WA].

8. *California Consumer Privacy Act (CCPA)*, STATE OF CALIFORNIA DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa [https://perma.cc/3QTW-ZWL2].

from the early 1900s to the 1970s.[9] The People's War was then enveloped under the umbrella of active defense from the late 1970s until the early 1990s.[10] Finally, China focused on warfighting under informal conditions from approximately the early 1990s onwards.[11] However, active defense remains an important underpinning of Chinese military doctrine and strategic policy and is "a fundamentally defensive political and strategic stance, enabled—when required—by operational and tactical offense," characterized by multi-layered defenses that an adversary must overcome, alongside a no first-strike policy.[12] Because such multi-layered defenses call for leveraging the skills of the civilian populace, a core component of active defense is the concept of the People's War, which also remains an underlying principle, even with doctrinal shifts throughout the years. The People's War developed from its roots as a struggle against the gentry to its modern iteration of a civil-military fusion that preserves certain key traits of the original idea, including capitalizing on asymmetrical advantages and sustaining a protracted war.

A. *Mobilizing the Masses*

Pre-1949, China's military doctrine was largely rudimentary, with basic military schooling and doctrinal development that often drew from foreign sources, though Mao Zedong's philosophy also developed during this time period and is closely associated with the People's War.[13] The concept of the People's War in China can be found as early as 1927, during which Mao identified the potential power in leveraging the peasant population in Hunan in a revolutionary struggle against the gentry, deemed a powerful, oppressive social class that needed to be overthrown to ensure to the well-being of the masses.[14]

Initially, at an operational level, the emphasis was on organizing and consolidating the strength of the masses against an enemy so that "several hundred million peasants will rise like a mighty storm, like a hurricane, a force so swift and violent that no power, however great, will be able to

---

9. 1 MAO ZEDONG, SELECTED WORKS OF MAO TSE-TUNG 23 (1st ed. 1965); NGOK LEE, THE CHINESE PEOPLE'S LIBERATION ARMY 1980-82: MODERNISATION, STRATEGY AND POLITICS 50–51 (1983).

10. LEE, *supra* note 9, at 50–51; M. TAYLOR FRAVEL, CHINA'S MILITARY STRATEGY SINCE 1949 220 (2019).

11. FRAVEL, *supra* note 10, at 220.

12. *Zhongguo de Junshi Zhanlue* (*中国的军事战略*) [*China's Military Strategy*], GUOWUYUAN XINWEN BANGONGSHI (国务院新闻办公室) [STATE COUNCIL INFORMATION OFFICE], June 2015, http://www.scio.gov.cn/zfbps/ndhf/2015/Document/1435161/1435161.htm [https://perma.cc/G75R-BYZB]; Chinese Tactics, Army Techniques Publication, No. 7-100.3, 1-7 (Aug. 2021).

13. KA PO NG, INTERPRETING CHINA'S MILITARY POWER: DOCTRINE MAKES READINESS 49 (1st ed. 2004); FRAVEL, *supra* note 10, at 220.

14. ZEDONG, *supra* note 9.

hold it back."[15] Mao further noted in 1938, "Mobilization of the common people will create a vast sea in which to drown the enemy, create the conditions that will make up for our inferiority in arms and other things, and create the prerequisites for overcoming every difficulty in the war."[16]

While Mao reiterated the concept of the People's War throughout his written works, the term itself did not officially appear until Mao's political report to the Seventh National Congress of the Communist Party of China in 1945.[17] In his report, Mao stated that "all the anti-Japanese people in the Liberated Areas of China are called upon to join organizations of workers, peasants, youth and women, and cultural, professional and other organizations, which will wholeheartedly perform various tasks in support of the armed forces . . . [s]uch is a real people's war."[18] Additionally, Mao anticipated that a People's War would be a protracted war, one that—even where enemy forces struck deep into the mainland—there would be constant pockets of resistance, as the mobilized masses would gradually reinforce its main fighting effort to strain the enemy "under the trial of innumerable battles."[19] Though warfare in China shifted from a revolutionary movement against the gentry in Hunan to national liberation from the Japanese under the Second Sino-Japanese War, the core concept of the People's War remained the same—mobilization of the masses against a superior enemy to mitigate imbalances in military strength and to supplement the conventional army's warfighting functions in areas such as intelligence and logistical support.

B. *Active Defense*

The People's War shifted to a national strategic level by the late 1970s to the early 1980s, under the guideline of active defense, in response to the threat of a Soviet incursion into China and the 1973 Arab-Israeli War, wherein the United States and the Soviet Union employed advanced weaponry, marking a shift in the modernization of warfare.[20] The Central Military Commission (CMC) approved active defense in 1980 and focused on establishing a multi-layered defense—to include forward defensive positions—that the enemy must overcome so that China has time to mobilize its forces.[21]

However, the People's War remained necessary due to concerns regarding asymmetrical capabilities against adversaries. Specifically, the

15. *Id.*
16. 2 MAO ZEDONG, SELECTED WORKS OF MAO TSE-TUNG 154 (1st ed. 1965).
17. 3 MAO ZEDONG, SELECTED WORKS OF MAO TSE-TUNG 213 (1st ed. 1965).
18. *Id.* at 216–17.
19. MAO, *supra* note 19, at 188.
20. LEE, *supra* note 9, at 50–51; FRAVEL, *supra* note 10, at 456.
21. FRAVEL, *supra* note 10, at 454–66.

Soviet Union's defense capabilities surpassed China's during this time, and cuts to China's defense budget in favor of economic development further hindered the country.[22] In the post-Mao era and in recognition of the evolution of warfare, Deng Xiaoping preserved the link to Mao's interpretation of the People's War, emphasizing that "we can defeat a superior enemy with inferior equipment, for our wars are just, they are people's wars."[23] Under Deng's leadership, active defense focused on conventional forces that were directly supported by the mobilized masses in the form of militia.[24] For example, during this time, sixty percent of the People's Liberation Army relied on austere support systems, which materialized as regional militia providing logistical support by drawing from local resources such as truck transportation.[25] Active defense thus marks a strategic shift in warfighting philosophy that continues to this day; civil resources directly supplement the conventional military as an integral part of combat operations, resulting in a deterring effect given the whole-of-society approach and layered defenses.[26]

C. *Modern Defense Approaches*

With the advent of modern technology in the 1990s, the People's War transformed again into a concept that promoted close integration of the military and civilian sectors, with the rationale of fortifying military strength with commercial capabilities.[27] The CMC adopted a new strategic guideline in 1993 titled "winning local wars under modern,

22. LEE, *supra* note 9, at 50. Of note, in the late 1970s, a point of critique was whether the People's War was still relevant in light of future wars given technological advancements. Given such advancements, tactics that were previously successful, e.g., throwing grenades into sight openings on armored vehicles, may no longer be valid. Indeed, Su Yu, the commissar and party secretary of the Academy of Military Science beginning in 1972, felt that the People's War had largely been relegated to an abstract slogan. FRAVEL, *supra* note 10, at 472–75.

23. DENG XIAOPING, SELECTED WORKS OF DENG XIAOPING: VOLUME II (1975-1982) (1995).

24. FRAVEL, *supra* note 10, at 230. Beginning in 1978, the Central Committee of the Chinese Communist Party renewed focus on mobilization of people in warfare as militiamen, formalizing training and doctrine, e.g., having a separation of roles for urban and rural militia, where—for instance—the main effort for urban militia would be to construct city defenses. LEE, *supra* note 9, at 80–81.

25. LEE, *supra* note 9, at 73–75.

26. Chinese Tactics, *supra* note 12, at 1–7.

27. The term military-civil fusion and its various iterations can be found as far back as the Mao Zedong era as the basis of the People's War, i.e., making use of the civilian sector for warfighting, but in contrast to its initial inception that focused on mobilization of the peasantry, military-civil fusion in the modern day identifies the need for a symbiotic relationship between the military and civilian sectors, particularly within areas of technological development in which military and civilian technology should be mutually compatible. Jiang Ying (江英), *Jicheng Fazhan Junmin Shendu Ronghe Guangrong Chuantong* (*继承发展军民深度关荣传统*) [*Inherit and Develop the Glorious Tradition of Deep Military-Civil Fusion*], GUANGMING RIBAO (光明日报) [GUANGMING DAILY] July 18, 2017, https://epaper.gmw.cn/gmrb/html/2017-07/18/nw.D110000gmrb_20170718_2-02.htm [https://perma.cc/6PM8-6HR4].

high-technology conditions," largely in response to the Gulf War, which saw the use of precision-guided munitions, again signaling a shift in the advancement of warfare—in particular, technological augments to maneuver forces.[28] Indeed, against predictions by Chinese military analysts that the Gulf War would result in a protracted war, the United States and allied countries defeated the Iraqi military within one hundred hours from the start of the conflict, thus serving as a catalyst for change in Chinese military strategy.[29]

1. Warfighting Under "Informatization"

The 1993 guideline focused on developing a new approach to warfighting that combined an array of systems, e.g., precision-guided weapons, intelligence, and electronic, given that modern warfare was no longer strictly confined to targeting the forward line of troops or the support area; instead, attacks could also target information hubs and operational systems.[30] However, the 1993 guideline nevertheless remained rooted in the concept of active defense, honing in on regional, localized disputes along China's borders and regions, e.g., Taiwan, as opposed to a broader enemy invasion of mainland China.[31] Zhang Wangnian, the general chief of staff, acknowledged the challenges of warfighting given new technologies and the struggles of "being rooted in using inferior equipment to defeat an enemy."[32]

To remedy these obstacles while also adhering to active defense as a foundational strategy, Zhang proposed an emphasis on the mobility of naval, air, and missile forces to rapidly react to threats in addition to the development of advanced weaponry.[33] China further made minor adjustments to its military strategy in 2004 and 2014, with the 2004 strategy focusing on addressing informatization—the prevalence of information technology throughout all aspects of military operations—and the 2015 strategy focusing on integrated joint operations in addition to informatization, marking the continued recognition of the importance of technology and information.[34]

2. Civil-Military Fusion

While military strategies from 1993 onwards placed an emphasis on conventional military and multi-domain operations, the People's War remained a crucial principle, evolving from the organization of the

28. FRAVEL, *supra* note 10, at 590–94.
29. *Id.* at 608–09.
30. *Id.* at 618.
31. *Id.* at 599–600.
32. *Id.* at 651.
33. *Id.* at 651–52.
34. *Id.* at 699–702.

masses in the early 1900s into the concept of military-civil fusion in the modern day, echoing the whole-of-society approach of active defense.[35]

Military-civil fusion has numerous concepts, connotations, and nuances as it developed over a number of years but can be broadly understood as the integration and pairing of the civilian sector with the military with the goal of more effective warfighting.[36] One such term for military-civil fusion is *junmin jiehe*, or "combining the military and civilian sectors," which originated with Deng in 1978 as a strategy whereby—in a hands-off approach—the government encouraged the development of dual-use technologies in the 1980s.[37] Crucially, in the 1990s, alongside the 1993 strategic guideline, the government began to take an active role in the development of dual-use technologies, such as by providing defense firms with financial assistance and appropriate networking for creating such technologies.[38] Finally, the late 1990s saw a further increase in the importance of integrating the military and civilian sectors, as demonstrated by one of the key policy objectives of the Commission of Science, Technology, and Industry for National Defense, which highlighted "two-way civil-military technology cooperation, transfers, promotions, and joint development."[39]

The People's War ultimately persisted within Chinese military strategy across two centuries. It underwent a transformation from more political origins in leveraging the proletariat against the gentry, to a whole-of-society, layered defense approach that uses a close relationship between the military and civilian sectors, especially concerning technological integration. Modern Chinese doctrine retains aspects of the People's War, including asymmetrical warfare and "long-term combat [that] consumes the enemy in protracted contests."[40]

II. THE ADVENT OF CYBERSPACE

The development of cyberspace further changed the nature of warfare and is now largely considered a new warfighting domain or dimension.[41]

---

35. *Id.* at 231.

36. ALEX STONE, MILITARY-CIVIL FUSION TERMINOLOGY: A REFERENCE GUIDE 6–8 (2021).

37. *Junmin jiehe* contained four key principles: (i) developing dual-use technologies, (ii) ensuring that peacetime development took into account wartime mobilization, (iii), prioritizing military research and development in the civilian economy, and (iv) allowing the military to benefit from the effects of economic prosperity. TAI MING CHEUNG, FORTIFYING CHINA: THE STRUGGLE TO BUILD A MODERN DEFENSE ECONOMY 8 (2009).

38. CHEUNG, *supra* note 37, at 8.

39. *Id.*

40. *See generally* JUNSHI KEXUEYUAN (军事科学院) [ACADEMY OF MILITARY SCIENCE], ZHANLUE XUE (战略学) [SCIENCE OF MILITARY STRATEGY] (2020).

41. "Cyberspace is a global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and

China has recognized the importance of cyberspace, particularly in light of the proliferation of network connectivity and threats from geopolitical rivals and hackers. Indeed, the United States elevated its Cyber Command to the tenth Combatant Command in 2018.[42] Other countries, including the United Kingdom, France, and Japan, have followed suit, bringing cyber capabilities to a national strategic level and holding exercises that test offensive and defensive capabilities in cyberspace.[43] With over 730 million mobile internet users and 1.94 million network terminals infected with viruses per month within China, cyberspace has become a major concern for Chinese national security.[44] Despite the unique characteristics of cyberspace as a warfighting domain, the concept of the People's War under active defense holds lasting relevance in understanding China's approach to cyber operations.

In the past three decades, China has placed increased importance on informatization and cybersecurity in recent years. In China, cyber operations fall under the broader umbrella of information operations, which also includes other functions such as military information support operations and electronic warfare.[45]

Chinese scholars and military institutions have long forecasted cyberspace to be a new warfighting domain. A People's Liberation Army publication noted in 2006 that the twenty-first century is the century of information warfare; with over 170 countries and regions connected via computer networks, which can be attacked, cyberspace is the new combat space.[46] The Academy of Military Science further emphasized that

---

controllers." Operations, Field Manual No. 3-0, paragraph 1–31 (Dec. 6, 2017). "Cyberspace is highly vulnerable for several reasons, including ease of access, network and software complexity, lack of security considerations, in network design and software development, and inappropriate user activity." *Id.* at 1–33.

42. Li Minghai (李明海), *Wangluo Xinxi Tixi Junmin Ronghe Zhanlue de Sikao* (*网络信息体系军民融合战略的思考*) [*Reflections on the Strategy of Civil-Military Integration of Information Network Systems*], WANGLUO CHUANBO ZAZHI (网络传播杂志) [J. NETWORK COMMUNICATION], June 12, 2018, http://www.cac.gov.cn/2018-11/12/c_1123701001.htm [https://perma.cc/5ZFT-AXZC].

43. *Id.*

44. *Id.*

45. AMY CHANG, WARRING STATE: CHINA'S CYBERSECURITY STRATEGY 13 (2014). There are grounds for noting a possible semantic distinction in China's use of the word "cyber." *Id.* Because references to the cyber domain are noted in terms of *wangluo*, or network, in China, some scholars argue that network security or network space are more appropriate terms to avoid possible divergences in meaning. *Id.* In common parlance, however, Chinese media largely does not make the same distinction between the two terms. *See, e.g.*, *China's First Data Security Law and its Wider Impact*, CGTN, Sept. 7, 2021, https://news.cgtn.com/news/2021-09-07/China-s-first-data-security-law-and-its-wider-impact-13lgE8ufFsI/index.html [https://perma.cc/R6HV-RCVY].

46. *Lun Xin Shiji Xin Jieduan Wo Jun De Lishi Shiming* (*论新世纪新阶段我军的历史使命*) [*Regarding the Historical Mission of our Army in the New Century and Era*], Jiefangjun Bao

developing cyber capabilities is a priority, particularly because networks inevitably have vulnerabilities, and cyber defense can be difficult because of the numerous vulnerabilities that have yet to be identified.[47]

China's cyber concerns are elevated in light of numerous cybersecurity incidents, ranging from small data breaches to attacks on government networks. In 2011, unidentified foreign entities used the Indian government's National Informatics Centre servers to attack Chinese government servers.[48] In 2020, the coronavirus pandemic leaked the personal information of four to five hundred travelers from Wuhan, China, after submission to regulators and transportation entities.[49] More recently, in 2022, unknown hackers stole over 23 terabytes of personal information from the Shanghai police database, resulting in the largest cyberattack in Chinese history.[50] Over the past few years, China incurred over 2,700 advanced cyberattacks against a wide range of industries, spanning from scientific research institutions to major internet companies.[51]

The People's War persists even within the realm of cyberspace through the framework of active defense. The Science of Military Strategy (SMS), a doctrinal publication of the People's Liberation Army, addressed guidance for cyberspace for the first time in its 2013 edition and reiterated the concept of active defense.[52] The SMS contrasted China's military deterrence with those of Western countries, noting that rather than projecting military power to further global hegemony, China is defensively postured—adhering to the concept of active defense to

---

(解放军报) [PLA DAILY], Jan. 9, 2006, http://news.sohu.com/20060109/n241350798.shtml [https://perma.cc/LVH8-K9FR].

47. JUNSHI KEXUEYUAN (军事科学院) [ACADEMY OF MILITARY SCIENCE], *supra* note 40, ZHANLUE XUE (战略学) [SCIENCE OF MILITARY STRATEGY] 193 (2013).

48. Josy Joseph, *Govt Servers Used for Cyber Attacks on China, Other Countries' Networks*, TIMES OF INDIA (Nov. 17, 2011), https://timesofindia.indiatimes.com/tech-news/govt-servers-used-for-cyber-attacks-on-china-other-countries-networks/articleshow/10760699.cms [https://perma.cc/2EPB-55CF].

49. Yan Luo, *Cyberspace Administration of China Releases Notice on the Protection of Personal Information in the Fight Against Coronavirus*, INSIDE PRIVACY (Feb. 11, 2020), https://www.insideprivacy.com/international/china/cyberspace-administration-of-china-releases-notice-on-the-protection-of-personal-information-in-the-fight-against-coronavirus/ [https://perma.cc/98XV-MGND].

50. *China's Cabinet Stresses Cybersecurity After Data Leak*, BLOOMBERG (July 6, 2022), https://www.bloomberg.com/news/articles/2022-07-07/china-s-cabinet-urges-greater-cyber security-after-mass-data-leak [https://perma.cc/6JL4-7XJF].

51. *Over 2,700 Cyber Attacks Launched Against China, Chinese Security Company 360 Found*, GLOBAL TIMES (Mar. 4, 2021), https://www.globaltimes.cn/page/202103/1217364.shtml [https://perma.cc/P2EB-E2GK].

52. JUNSHI KEXUEYUAN (军事科学院) [ACADEMY OF MILITARY SCIENCE], *supra* note 40, at 145.

contain crisis and counteract invasion actions from other countries that may infringe on China's interests.[53]

In both the 2013 and 2020 editions of SMS, active defense entailed close cooperation between the political and civilian fields and the differing warfighting functions.[54] To this end, the General Secretary of the Chinese Communist Party, Xi Jinping, stated in a 2016 conference that the party, the country, the army, and individuals of all ethnic groups should move forward with one heart and one mind to overcome obstacles, setting forth another iteration of *junmin jiehe*, an echo of the People's War.[55] Specifically, within the cyber realm, Li Minghai, the deputy director of the War and Crisis Response Training Center, noted that close integration of military and civilian information systems is the foundation of victory in that it creates a joint force to respond to threats against networks.[56] To address cyberspace's challenges as a new warfighting domain, China thus continued its doctrinal legacy of a whole-of-country approach in unifying the military and civilian sectors to ensure a multi-layered defense.

III. CHINA'S CYBERSECURITY LAW AND IMPLEMENTING REGULATIONS

In conjunction with rising cybersecurity concerns and challenges, China has promulgated laws and guiding strategies to shape and secure its interests in cyberspace, with the view that there is no national security without cybersecurity.[57] As early as 2003, China published Document 27, also known as the Opinions of the Leading Group for Strengthening Information Security Assurance Work, which laid the groundwork for dynamic monitoring of the internet and protecting critical infrastructure.[58] By 2011, China's foray into data security at the national level was imminent, as the Ministry of Information and Industry Technology, China's internet regulator, issued guidelines for protecting

53. *Id.*

54. JUNSHI KEXUEYUAN (军事科学院) [ACADEMY OF MILITARY SCIENCE], *supra* note 28, at 33 (2020); JUNSHI KEXUEYUAN (军事科学院) [ACADEMY OF MILITARY SCIENCE], *supra* note 40, at 148.

55. *Xi Jinping: Jianchi Jun di Heli Junmin Tongxin Quanmian Tigao Shuang Yong Gongzuo Shuiping* (*习近平：坚持军地合力军民同心 全面提高双拥工作水平*) [*Xi Jinping: Sustain the United Efforts of the Military and the People, Raise the Quality of Dual-Use Efforts*], XINHUA SHE (新华社) [XINHUA NEWS], July 29, 2016, http://www.xinhuanet.com/politics/2016-07/29/c_1119306354.htm [https://perma.cc/3XH9-HWL6].

56. Li Minghai (李明海), *supra* note 42.

57. Hawke Johannes Gierow, *Cybersecurity in China: New Political Leadership Focuses on Boosting National Security*, MERCATOR INST. FOR CHINA STUDIES: CHINA MONITOR 2 (Dec. 9, 2014), https://merics.org/sites/default/files/2020-05/China_Monitor_20_Cyber_Security-National_Security_EN.pdf [https://perma.cc/UY8E-SHLS].

58. Adam Segal, *China Moves Forward on Cybersecurity Policy*, CFR (June 24, 2012), https://www.cfr.org/blog/china-moves-forward-cybersecurity-policy [https://perma.cc/RU7S-UBEV].

personal information; though the guidelines did not have the force of law, they nevertheless paved the way for a legal regime that responds to the evolving cyber environment via national standards.[59]

In 2016, the National People's Congress enacted the CSL, which came into effect in 2017 and was a landmark legislation that aimed to strengthen data protection to further national security. Importantly, it is the "first Chinese law that systematically lays out the regulatory requirements on cybersecurity, subjecting many previously under-regulated or unregulated activities in cyberspace to government scrutiny."[60]

In contrast to other data protection regulations, such as the GDPR or CCPA, which emphasize privacy and personal information protection, the CSL's foremost focus is on national security.[61] For example, the CSL seeks to impose security obligations on network operators, critical information infrastructure, and cross-border transfers of data; the broad applicability of concepts and terms within the CSL has the effect of exerting more control over data and information infrastructure, both foreign and domestic.[62] The CSL is accompanied by numerous other regulations that further clarify differing aspects and definitions within the field of data security. In particular, the Data Security Law regulates data processing activities with implications on national security, and the Personal Information Protection Law governs the protection of personal information, thereby "form[ing] an over-arching framework that will govern data protection and cybersecurity in China for years to come."[63]

The promulgation of the CSL and its implementing regulations drew a quick response from multinational corporations, particularly those with

---

59. *Release of China's First Personal Information Protection Standards Imminent*, INSIDE PRIVACY (Aug. 8, 2011), https://www.insideprivacy.com/international/release-of-chinas-first-personal-information-protection-standards-imminent [https://perma.cc/75MQ-B3C6].

60. *China Passes New Cybersecurity Law*, INSIDE PRIVACY (Nov. 8, 2016), https://www.cov.com/-/media/files/corporate/publications/2016/11/china_passes_new_cybersecurity_law.pdf [https://perma.cc/XYM4-NJ9Y].

61. The United States has responded to cyber challenges through executive and legislative means, such as the Biden Administration's Executive Order entitled "Improving the Nation's Cybersecurity," and noted the need for better communication between the public and private sectors, but the area of cybersecurity and privacy is largely covered by a patchwork of laws at the state and federal level, as opposed to having a broad, unified standard. Alan C. Raul and Snezhana S. Tapia, *In a Nutshell: Data Protection, Privacy, and Cybersecurity in USA*, LEXOLOGY (Nov. 5, 2021), https://www.lexology.com/library/detail.aspx?g=1df08bf2-622a-4674-ac31-51930f6a80f8 [https:// perma.cc/67FC-37AH].

62. *China Passes New Cybersecurity Law*, *supra* note 60.

63. *China Released Updated Draft Data Security Law and Personal Information Protection Law for Public Comments*, INSIDE PRIVACY (May 3, 2021), https://www.cov.com/-/media/files/corporate/publications/2021/05/covington-alert--china-released-updated-draft-data-security-law-and-personal-information-protection-law-for-public-comments-may-3-2021.pdf [https://perma.cc/S9SM-7RKW].

a significant online presence. Corporations from over forty countries issued a letter to Chinese premier Li Keqiang, with concerns including an assertion that regulator-led security reviews of information technology products and services under the CSL only create additional barriers to entry as opposed to heightened data security.[64] Despite an initial barrage of protests, corporations ultimately moved forward with regulatory compliance, given a heightened awareness of customer privacy rights during that time, in light of the passage of numerous privacy laws with global impacts, such as the GDPR. Major law firms pivoted towards establishing data privacy and cybersecurity practice groups to ease the transition towards compliance and redesigning privacy policies for corporations. Nevertheless, while Chinese regulators emphasized that the CSL's goal was to promote national security and safeguard the public's interests with a significant consumer privacy component, the CSL, at its core, reflects the government's focus on improving a defensive cyber posture, with key elements of the People's War in play—a whole-of-country defense, the ability to sustain a protracted war, and asymmetrical warfare.[65]

A. *Whole-of-Country Defense*

The CSL and accompanying regulations contain numerous provisions that set forth a broadly applicable security standard for all entities operating within the country. Article 21 provides that "[n]etwork operators shall perform . . . security protection duties according to the requirements of the cybersecurity multi-level protection system," with network operators broadly defined as "network owners, managers, and network service providers."[66] Additionally, Article 31 states that "[t]he State implements key protection on the basis of the cybersecurity multi-level protection system for public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people's livelihood, or the public interest."[67] Finally, as both articles allude to, the

64. Tom Mitchell and Shawn Donnan, *Chinese Laws Prompt Global Business Backlash*, FIN. TIMES (Aug. 11, 2016), https://www.ft.com/content/8103baa0-5f9c-11e6-ae3f-77baadeb1c93 [https://perma. cc/H9R8-MQH6].

65. Charles Clover and Sherry Fei Ju, *China Cyber Security Law Sparks Foreign Fears*, FIN. TIMES (Nov. 7, 2016), https://www.ft.com/content/c330a482-a4cb-11e6-8b69-02899e8bd9d1 [https:// perma.cc/BB2P-KDYG].

66. Rogier Creemers, et al., *Translation: Cybersecurity Law*, DIGICHINA (June 29, 2018), https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017 [https://perma.cc/9YBL-RUW4].

67. *Id.*

multi-level protection system exists as a tiered system of classifying information systems and imposes security standards based on the risk and impact of a possible data breach.

In line with the People's War and the idea of civil-military unity, the CSL's expansive provisions in subjecting network operators and critical information infrastructure to common security standards further China's strategy of mobilizing the entirety of society in a defensive posture to minimize weaknesses across all networks within the country. The term network operator "covers virtually any business that operates an internal computer network, or even just a website, in China."[68] In other words, the CSL applies not only to government-operated networks but also to private-sector networks that belong to foreign and domestic companies.

All entities that operate a network in China are now required to adhere to security standards that assess the impact on national security, public interests, or social order, evaluated at a scale of one to five, with the most stringent standards applicable to network operators that pose the highest risk at level five.[69] Such standards range from requiring a qualified expert to conduct a security review of level two networks to requiring regulatory intervention in determining a schedule for reevaluating level five networks, which are often government-owned.[70] The broadly applicable wording with respect to network operators and the unified security standards of the CSL reflect the spirit of civil-military fusion because public and private network operators are equally obligated to implement cybersecurity measures, thus reducing reliance on purely governmental or military networks for national security and defense. Additionally, a whole-of-country defense that utilizes the civilian sector is important to reducing potential weaknesses in critical industries.[71]

This concern manifested in practice during large-scale combat operations in 2022, as Russia conducted a series of offensive cyber

---

68. Zachary S. Brez, et al., *Challenges and Advice for Multinational Companies in Complying with Chinese Cybersecurity Law*, KIRKLAND & ELLIS (Feb. 23, 2018), https://www.kirkland.com/publications/article/2018/02/challenges-and-advice-for-multinational-companies [https://perma.cc/P5ZM-WC7J].

69. U.S.-China Business Council, *The 5 Levels of Information Security in China*, CHINA BUS. R. (Dec. 5, 2016), https://www.chinabusinessreview.com/the-5-levels-of-information-security-in-china [https://perma.cc/TBZ4-ZQ2G].

70. Michael Pang and Jonathan Hsieh, *China's Cybersecurity Law: Multiple-level Protection Scheme*, PROTIVITI, https://www.protiviti.com/HK-en/insights/pov-multiple-level-protection-scheme [https://perma.cc/4QAD-Y6VY].

71. "Unlike military or intelligence networks, which are defended and overseen by the Department of Defense, or various civilian government networks, which are defended and overseen by the Department of Homeland Security, the National Institute of Standards and Technology, and the Office of Budget and Management, no one entity defends the private networks that most critical infrastructure relies upon." Robert K. Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor"*, 18 VA. J.L. & TECH. 289, 293 (2014).

operations against Ukrainian critical infrastructure, a mix of government and civilian systems, including targeting a power plant in an attempt to hinder electricity distribution and government websites from delaying distribution of relief supplies.[72] By imposing heightened cybersecurity obligations on critical information infrastructure, alongside bringing all network operators under the CSL's scope, China would be able to bolster its cybersecurity capabilities by mobilizing all entities operating within the country, thereby minimizing areas that may be vulnerable to exploitation.

B. *Protracted War – Big Areas and Little Areas*

In addition to the CSL, Chinese regulators have also promulgated a plethora of sector-specific cybersecurity requirements that further elevate its ability to withstand cyberattacks and address vulnerabilities. For example, in October 2019, the National People's Congress enacted the Encryption Law, which imposes, among other requirements, the obligation for critical information infrastructure operators to undergo a security assessment of commercial encryption product usage, where applicable, as well as an import-export framework that restricts encryption products that may impact national security.[73] In February 2020, the People's Bank of China issued the Personal Financial Information Protection Technical Specification, which governs how financial institutions collect and process personal information; e.g., where sensitive information is transmitted over public networks, financial institutions must ensure that such information is encrypted.[74] The aforementioned laws are a sampling of the sector-specific cybersecurity requirements that have been promulgated on top of the CSL and demonstrate China's commitment to additional security measures for sectors of concern, with some overlap with critical information infrastructure.

Sector-specific laws in the areas including encryption and finance allow for heightened protection of certain sectors that the government deems sensitive. Interconnectivity is a key nature of cybersecurity, which means that "[w]hile interdependencies among CI [critical infrastructure]

---

72. Jakub Przetacznik and Simona Tarpova, *Russia's War on Ukraine: Timeline of Cyber-attacks*, EPRS (June 2022), https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/ EPRS_BRI(2022)733549_EN.pdf [https://perma.cc/E67W-GFY4].

73. Eric Carlson and Yan Luo, *China Enacts Encryption Law*, INSIDE PRIVACY (Oct. 31, 2019), https://www.insideprivacy.com/data-security/china-enacts-encryption-law/ [https://perma.cc/2WCC-B5XM].

74. Yan Luo, *China Releases Personal Financial Information Protection Technical Specification*, INSIDE PRIVACY (Dec. 2, 2019), https://www.insideprivacy.com/international/china/china-releases-personal-financial-information-protection-technical-specification/ [https://perma.cc/5E8N-S5ER].

are often necessary to meet design specifications, they also lead to undesirable situations when a fault or attack occurs in one CI and escalates to other connected CI."[75] A case study was done regarding the impact of a cyberattack on interconnected systems of a water distribution center and a water treatment plant.[76] Here, after acquiring knowledge of points of weakness in the two systems, an attacker can manipulate multiple points simultaneously, with a larger number of interconnected nodes or links translating into a larger potential surface area for attack.[77]

The interconnectivity of systems can also mean that a single vulnerability can affect a multitude of systems and infrastructure. In January 2003, the SQL Slammer worm exploited unpatched SQL servers; an infected server would then prompt the host computer to search for and infect additional servers.[78] This cascading effect from a single point of weakness resulted in severe consequences, including ATM failures and canceled flights.[79] The sector-specific cybersecurity laws that exist on top of the CSL mitigate the dangers of such cascading effects of a cyberattack. For example, an attack on a specific node in one sector may be isolated, thus keeping the other sectors and the larger cyberinfrastructure intact.

The differing, heightened requirements across sectors lend to the concept of "big areas versus little areas" under the People's War, in which even if the enemy conquers and occupies a specific area of the country, the larger, remaining areas remain intact and in China's possession, with the latter continuously mobilizing to maintain sustained resistance against the enemy.[80] This would also allow China to fight a protracted war of attrition against a much stronger enemy by having constant pockets of defense.[81] By extension, China's sector-specific cyber regulations in conjunction with the CSL would, in theory, allow it to survive an initial cyberattack by limiting its impact and preserving the integrity of its remaining systems to fight a protracted war.

---

75. Venkata R. Palleti, et al., *Cascading Effects of Cyber-attacks on Interconnected Critical Infrastructure*, CYBERSECURITY 2 (Mar. 1, 2021), https://cybersecurity.springeropen.com/track/pdf/10.1186/s42400-021-00071-z.pdf [https://perma.cc/RRW8-UCZ8].

76. *Id.*

77. *Id*. at 16–17.

78. Roger A. Grimes, *SQL Slammer 16 Years Later: Four Modern-Day Scenarios that Could be Worse*, CSO (Jan. 31, 2019), https://www.csoonline.com/article/3337179/sql-slammer-16-years-later-four-modern-day-scenarios-that-could-be-worse.html [https://perma.cc/TZJ8-7DJJ].

79. *Protecting Interconnected Systems in the Cyber Era*, PWC 11, https://gita.org.in/Attachments/Reports/Protecting%20interconnected%20systems%20in%20the%20cyber%20era.pdf [https://perma.cc/L4JN-EPPM].

80. MAO, *supra* note 19, at 147–48.

81. *Id.* at 141–42.

C. *Asymmetrical Warfare*

Chinese regulators have additionally set forth laws that provide for actively monitoring potential vulnerabilities. In 2021, the Cyberspace Administration of China and the Ministry of Public Security promulgated the Provisions on the Management of Network Product Security ("Network Product Security Provisions"), which requires reporting of security vulnerabilities.[82] Article 7 states that network operators and network product providers shall report the vulnerability to the Ministry of Industry and Information Technology within two days of discovering a security vulnerability.[83] Article 9 also prohibits entities and individuals from publishing vulnerabilities to overseas entities and individuals.[84] Like the CSL, the aforementioned Articles broadly apply to network operators and network product providers of hardware and software operating within China.[85] Separately, the Data Security Law requires processors of important data to submit a regular risk assessment report that includes "the types and amounts of important data processed, information on data processing, data security risks and the response measures for them."[86]

The Network Product Security Provisions and Data Security Law show China's concerns with an interest in zero-day vulnerabilities. Zero-day vulnerabilities are vulnerabilities that entities have not yet patched. Importantly, according to a case study done by a cyber threat company based on tracking sixty vulnerabilities that occurred between 2018 and 2019, "[t]he average day between disclosure and patch availability was approximately 9 days," thereby providing attackers with a window of opportunity to manipulate the vulnerability.[87] Moreover, forty-two percent of vulnerabilities were exploited even after a patch was issued.[88] By being able to monitor such zero-day vulnerabilities under the Network Product Security Provisions, as well as having risk assessment reports that detail data processing and its corresponding risks as mandated by the Data Security Law, China would have a better understanding of new

82. Wangluo Chanpin Anquan Loudong Guanli Guiding (网络产品安全漏洞管理规定) [Provisions on the Management of Network Product Security] (2021).

83. *Id.*

84. *Id.*

85. *Id.*

86. Data Security Law of the People's Republic of China (2021).

87. Kathleen Metrick et al., *Think Fast: Time Between Disclosure, Patch Release and Vulnerability Exploitation—Intelligence for Vulnerability Management, Part Two*, MANDIANT (Apr. 13, 2020), https://www.mandiant.com/resources/time-between-disclosure-patch-release-and-vulnerability-exploitation [https://perma.cc/GBH9-NVQR].

88. *Id.*

vulnerabilities as they arise to protect its own networks and potentially use them against adversaries in offensive cyber operations.[89]

This further aligns with a core tenet of the People's War: overcoming a superior adversary requires flexible tactics and exploiting the enemy's weaknesses through asymmetrical warfare.[90] The PLA has long framed military strategy from a position of needing to prevail over a militarily superior adversary, and knowledge of newly discovered, obscure vulnerabilities would—in theory—present an opportunity for an advantageous attack on such adversary's systems or software where a patch has either not yet been released, or alternatively, has been released but has not seen widespread distribution.[91] Of note, monitoring vulnerabilities can also be viewed under the broader umbrella of active defense. Given the lack of geographical boundaries within cyberspace, networks, and nodes can be construed as vulnerable to attack on the fringes of China's area of operations or territory. Such monitoring can be viewed as a forward defensive posture in providing early warning of possible weaknesses in cyberspace.

IV. U.S. STRATEGIC CONCERNS AND A PATH TO BRIDGING THE DIVIDE

The CSL sits at the intersection between military, civilian, and legal cyber interests, thus posing unique challenges to the United States in crafting an effective response. At the outset, the United States and China have differing views on their respective strategic approaches to cyber governance and cyber sovereignty, resulting in a higher possibility for misunderstandings or mistrust.[92] Moreover, while the United States should prioritize establishing a better system for sharing cyber-threat information in response to the CSL, the legislative process can be lengthy and needs to account for the competing interests of the public and private sectors.[93] A possible, more immediate path forward would be restarting high-level bilateral dialogues on cyber interests between the two countries to eliminate pockets of misunderstanding, establish red lines, and create a code of conduct to facilitate predictability in cyber operations further.

---

89. Brad D. Williams, *China's New Data Security Law Will Provide it Early Notice of Exploitable Zero Days*, BREAKING DEFENSE (Sept. 1, 2021), https://breakingdefense.com/2021/09/chinas-new-data-security-law-will-provide-it-early-notice-of-exploitable-zero-days [https://perma.cc/T7NB-ZA4L].

90. MAO, *supra* note 19, at 167.

91. Caitlin Campbell, *China's Military: The People's Liberation* Army, CRS 22 (June 4, 2021), https://sgp.fas.org/crs/row/R46808.pdf [https://perma.cc/48MQ-6YQ4].

92. Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 329 (2015); Anqi Wang, *Cyber Sovereignty at its Boldest: A Chinese Perspective*, 16 ISJLP 395, 397 (2020).

93. Palmer, *supra* note 4, at 197.

A. *A Fundamental Divide*

While in recent years, numerous countries have reached a consensus that cyberspace constitutes a new warfighting domain, the laws passed by each country regulating cybersecurity as it relates to national security ties into a broader issue of cyber governance.[94] From a Chinese perspective, cyberspace has intangible territorial borders that each country can exert control over for a number of goals, including the preservation of social stability, copyright protection, and national security; in other words, China promotes the concept of cyber sovereignty, which divides cyberspace into country-based jurisdictions.[95] Conversely, the United States prioritizes a free and open internet that embraces a multi-stakeholder approach to governance.[96] The advancement of cyber capabilities in both countries and the divergence in their strategic approach to cyberspace creates the potential for misunderstandings and, consequently, escalation of force.[97] For example, China may view the CSL as a legal framework that is necessary to safeguard its critical information infrastructure against malicious actors and possible foreign threats, but the United States may view the same law as destabilizing to the international community with respect to the free flow of information and also dangerous with respect to increasing its offensive cyber capabilities.[98] Indeed, even if a common interest in preventing escalation exists, the divergent views of cyberspace governance and strategy may result in what one party views as addressing legitimate domestic concerns as prepping the battlefield by another party.[99]

B. *Seeking Mutual Understanding of Strategic Interests in Cyberspace*

The United States has the challenge of formulating a balanced response to China's CSL, with the need to navigate the nuance between having an effective counter to the potentially offensive elements within the CSL and avoiding a spiral of mistrust and military escalation, as both

94. Eichensehr, *supra* note 92, at 329.

95. Wang, *supra* note 92, at 397.

96. Eichensehr, *supra* note 92, at 330.

97. Michael Kolton, *Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence*, 2 CYBER DEF. REV. 119, 137 (2017).

98. Laura Dobberstein, *China is Likely Stockpiling and Deploying Vulnerabilities, Says Microsoft*, REGISTER (Nov. 7, 2022), https://www.theregister.com/2022/11/07/china_stockpiles_vulnerabilities_microsoft_asserts [https://perma.cc/56B7-YQUC]; Tom Miles, *U.S. Asks China Not to Enforce Cyber Security Law*, REUTERS (Sept. 26, 2017), https://www.reuters.com/article/us-usa-china-cyber-trade/u-s-asks-china-not-to-enforce-cyber-security-law-idUSKCN1C11D1 [https://perma.cc/KSN3-6RQP].

99. Kolton, *supra* note 97, at 140.

countries would begin to enter into a feedback loop in responding to the other's actions.[100]

To mitigate the CSL's vulnerability reporting requirements, which can potentially be used offensively, the United States should continue its efforts in building a tailored, robust cyber-threat sharing framework between the public and private sectors to anticipate zero-day vulnerabilities similarly.[101] Real-time sharing and analysis of data trends and unusual behaviors would assist in identifying and stopping malicious activity.[102] To this end, the United States already has Information Sharing and Analysis Centers (ISACs), established by Presidential Decision Directive-63 in 1998, wherein "each critical infrastructure sector . . . establish[ed] sector-specific organizations to share information about threats and vulnerabilities," with most ISACs having "24/7 threat warning and incident reporting capabilities."[103] However, the effectiveness of ISACs remains questionable due to artificial self-imposed limits in cyber-threat sharing, where, for example, some ISACs share information only with trusted members, as opposed to allowing for broad, simultaneous dissemination of information.[104] A centralized entity or organization that aggregates and shares the cyber-threat information may be more effective in minimizing the shortcomings of the preexisting ISAC framework, particularly if the types of information to be shared is clearly delineated to filter for critical information and is screened to deconflict with the patchwork of applicable privacy laws.[105] However, a number of competing interests remain in play and have long hindered legislative progress in this area; whether the government should mandate information sharing or minimum security standards continues to be a point of contention.[106] Proponents of government-required standards believe that market forces and voluntary behavior are inadequate to address the cyber threats against the United States.[107] On the other hand,

100. *See, e.g.*, *id.* at 137.

101. Palmer, *supra* note 4, at 314.

102. *Id.* at 314–15.

103. *Id.* at 316; *About ISACs*, National Council of ISACs, https://www.nationalisacs.org/about-isacs [https://perma.cc/7UT5-NP49].

104. Palmer, *supra* note 4, at 317–18.

105. *Id.* at 355–56.

106. *Id.* at 297.

107. *Id.* Of note, under the Biden Administration, the United States government has taken steps to address collaboration between the public and private sectors; indeed, the United States government "announced and operated under a new model for cyber incident response by including private companies in the Cyber Unified Coordination Group." *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China*, WHITE HOUSE (July 19, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china [https://perma.cc/9WZ6-4QKB].

opponents of such standards believe that the government cannot effectively address the needs of varying industries and sectors and may stifle innovation instead.[108]

In light of the legislative and legal barriers that lengthen the timeline to establish an effective scheme of sharing cyber-threat information, a more immediate step the United States can take to address concerns surrounding the CSL would be to reestablish and participate in regular bilateral dialogue on cyber concerns, as well as create a code of conduct for cyber operations. The formal dialogue on cybersecurity that began under the Obama[109] and Trump[110] Administrations should continue to build a robust understanding of differing strategic interests and also enumerate the red lines that each country may have to prevent or deescalate potential crises in cyberspace. This is especially crucial in cyberspace, where the rapidness of a potential attack or response can come without the early warning signals of ground maneuver, such as troop buildup, and attribution can be unclear.[111] Accordingly, there must be a reversal of the current status, in which, after multiple years of the coronavirus pandemic, "many government channels [have been] canceled, suspended or lapsed, [and] unofficial dialogues have been among the few tools left to keep the two sides from continuing to talk past each other."[112] Importantly, the United States and China should agree on a code of conduct concerning cyber operations to further minimize areas of uncertainty. While the Tallinn Manual exists as what experts consider the "current black letter law on jus ad bellum and jus in bello rules relevant to cyber operations,"[113] some Chinese scholars[114] have been critical that the Tallinn Manual 2.0 does not adequately address

---

108. Palmer, *supra* note 4, at 297.

109. *First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes*, Dept. Justice (Dec. 2, 2015), https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0 [https://perma.cc/LT94-ETCU].

110. *First U.S.-China Law Enforcement and Cybersecurity Dialogue*, Dept. Justice (Oct. 6, 2017), https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue [https://perma.cc/A4H6-NSCS].

111. Ernest J. Monitz, et al., *U.S. Nuclear Policies for a Safer World*, NTI (June 10, 2021), https://www.nti.org/analysis/articles/us-nuclear-policies-safer-world [https://perma.cc/MVL4-N8Q2].

112. Christian Shepherd and Lyric Li, *China Wants to Mend Ties with the U.S. but it Won't Make the First Move*, WASH. POST (Nov. 13, 2022), https://www.washingtonpost.com/world/2022/11/13/china-united-states-relations-xi-jinping [https://perma.cc/V5VM-6824].

113. Ashley Deeks, *Tallinn 2.0 and a Chinese View on the Tallinn Process*, LAWFARE (May 31, 2015), https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process [https://perma.cc/XE8T-J5B9.

114. While such scholars may not necessarily represent the official views of the Chinese government or the People's Liberation Army, their views are nevertheless edifying in exploring how Chinese views may differ from Western views with respect cyberspace.

certain concerns, including the consequence-based view of cyberattacks[115] and data as a military objective.[116] The latter, in particular, has been controversial even between Chinese scholars who take differing stances on whether data should be considered a "non-object" military objective, in light of how the Tallinn Manual 2.0 considers military objectives to be objects, and even if it were to be considered a valid military objective, whether data should be segregated into military and civilian data.[117] Rather than simply following the Tallinn Manual 2.0, a code of conduct could codify the intent and stances of both governments and further explore red lines to reduce concerns of unintended or misinterpreted signals. Additionally, the less formal nature of a code of conduct, as compared with a treaty-based option, would be a good step forward in developing a better understanding of areas of concern with respect to cyber operations between the United States and China without locking either country into a potentially difficult political position.

CONCLUSION

Though the People's War has its origins in Mao Zedong's philosophy of class warfare in the early 1900s[118] and pre-dates the Second Sino-Japanese War, it has remained relevant in modern Chinese military doctrine as more than just an antiquated slogan. The People's War has evolved alongside doctrinal shifts throughout the decades, from active defense in the early 1970s[119] to fighting under informatized conditions in the early 1990s.[120] In this time, the People's War transformed from a more literal mobilization of the masses to overthrow the gentry into military-civil fusion under the umbrella of active defense.[121]

Even in the new cyber domain, the concept of the People's War is applicable and features heavily in the CSL. Indeed, the CSL's broadly mandated security standards across the public and private sectors[122] tie

115. The Tallinn Manual 2.0 takes a consequence-based view of cyberattacks, in which a cyber operation is considered a cyberattack where the operation is reasonably expected to cause death, damage, or injury to persons or objects. However, under this view, "assessment of the damage turns out to be extremely tricky, especially when the consequences are mostly indirect," and "the consequence-based approach limits the notion of the attack so as to exclude those operations that result in severe and disruptive non-physical harm." Zhixiong Huang and Yaohui Ying, *The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective*, 913 IRRC 335, 343 n.32 (2020).

116. *Id.* at 360.

117. *Id.* at 362–63.

118. Mao, *supra* note 12 at 23.

119. LEE, *supra* note 9, at 50–51.

120. FRAVEL, *supra* note 10, at 220.

121. *Id.* at 231.

122. *See, e.g.*, Creemers et al., *supra* note 66.

into the concept of a layered defense, using the strength of the entirety of the country under the People's War. Sector-specific regulations[123] on top of the CSL increase survivability through isolating threats, thereby setting conditions to fight a protracted war of attrition against the adversary. Finally, the CSL's vulnerability reporting mechanisms are suspected to have a secondary function of gathering zero-day vulnerabilities in an offensive capacity,[124] again tying into a familiar concept under the People's War—asymmetrical warfare, in which an adversary's weaknesses can be leveraged and exploited through non-conventional means.

In turn, the United States faces challenges in crafting a measured response to the CSL. A forceful response in shoring up offensive capabilities may not be ideal. Mike McConnell, a former director of the National Security Agency, noted:

> Let's say you take an action. We depend on this stuff more than anyone else. We're more vulnerable than anybody else in the world. If we could put a map of the world up here with the US on the center and we put bandwidth on top of it, it's a bell curve. Most of the communications in the world flow through the United States; we are the biggest users and beneficiaries. So, there's a great hesitancy to use anything in a cyber context because it's relatively easy to punch back aggressively.[125]

Additionally, in light of the legislative barriers to creating an effective cyber-threat information-sharing system,[126] the United States may find more immediate success in resuming high-level dialogue in identifying the red lines of each country and areas of potential misunderstanding, particularly as the United States and China have fundamental differences in their respective approaches to cyberspace and strategy. The United States should also formulate a bilateral code of conduct to eliminate further ambiguities in signaling and intent with respect to cyber operations, thereby reducing the risk of escalation. Notwithstanding the above, cyberspace will likely be a continued area of tension for the United States in the coming years, particularly with the increasing intersection between civilian and military purposes within cyberspace and the diverging views between countries with respect to cyber sovereignty.

---

123. *See, e.g.*, Carlson and Luo, *supra* note 84.

124. Dobberstein, *supra* note 98.

125. Kevin J. Deleney, Why the US Doesn't Use Cyber-weapons to Attack its Enemies More Often, QUARTZ (June 30, 2013), https://qz.com/99162/why-the-us-doesnt-use-cyber-weapons-to-attack-its-enemies-more-often-mike-mcconnell [https://perma.cc/UE67-GKSJ].

126. Palmer, *supra* note 4, at 297.