HACKING INTO CHINA'S CYBERSECURITY LAW

Jyh-An Lee[*]

China's Cybersecurity Law, which is thus far the most important internet legislation to be passed in the country, came into effect on June 1, 2017. The law has attracted significant attention and criticism from foreign companies. Although the Chinese government claims that the Cybersecurity Law will help reduce the risk of cyberattacks and safeguard national security, some critics believe that the law will further erode internet freedom in China. In particular, concerns have been raised that the law may not effectively enhance China's current level of cybersecurity but instead may be used to facilitate government censorship and surveillance, to increase unnecessary business operating costs, to steal intellectual property from foreign companies, and to protect domestic industries from global competition.

This Article provides a thorough analysis of important provisions of the Cybersecurity Law as well as their policy implications. It views the Cybersecurity Law as part of a broader set of policy steps that have been taken to streamline laws concerning the internet and national security. The law

* Associate Professor, Faculty of Law, The Chinese University of Hong Kong. I would like to thank Rehan Abeyratne, Gillian Bolsover, Anatole Boute, Bernard Chao, Shun-Ling Chen, Yu-Jie Chen, Wen-Tsong Chiou, David Donald, Yu Hong, Stuart Hargreaves, Gus Hurwitz, Lianrui Jia, Min Jiang, Jae Woon Lee, Wanbil Lee, Yu-Hsin Lin, Tzu-Yi Lin, Noam Noked, Tokunbo Ojo, Jeffrey Ritter, Lotus Ruan, Dini Sejko, Hsi-Ping Schive, Yen-Tu Su, Dicky Tsang, Felix Wu, Dwayne Winseck, Peter Yu, and Wolfgang Zankl for their helpful comments. This Article has also benefited from feedback provided in the 2017 Internet Law Works-in-Progress Conference at Santa Clara Law School, the 15th Chinese Internet Research Conference: "Divergence and Convergence in China's Internets" at Texas A&M University School of Law, Faculty Seminar at the Institutum Iurisprudentiae, Academia Sinica (IIAS) in Taipei, Faculty Research Seminar at The Chinese University of Hong Kong Faculty of Law, "iEthics-Cyberport Symposium on Data Privacy Protection and Cybersecurity" in Hong Kong, and the "Global Media Forum: Changes and Adaptations: Chinese Media and its Global Development" workshop at York University in Toronto. I also thank Agnes Cheung, the Legal Resources Librarian for her invaluable assistance. I am grateful to the editors of the *Wake Forest Law Review* for their extraordinary editorial support. The study underlying this Article was supported by a grant from the Research Grants Council in Hong Kong (Project No.: CUHK 14612417).

fulfills China's persistent aim to assert its internet sovereignty by imposing heavy obligations on network operators and critical information infrastructure operators. This Article contends that the law should be understood from the perspective of China's unique conception of cybersecurity and human rights. As cybersecurity is defined much more broadly in China than it is in the Western world, any digital information threatening social or political stability will be viewed as a cybersecurity, or even a national security, concern. This explains why the scope of the Cybersecurity Law is unprecedented. Moreover, the treatment of personal information in the Cybersecurity Law reflects China's human rights philosophy. While individuals enjoy a certain degree of human rights protection, those rights do not effectively protect them from government action.

TABLE OF CONTENTS

I. INTRODUCTION

Due to the pervasive use of the internet and digital technologies in both the private and public sectors, and the vulnerabilities of these technologies, cybersecurity has lately become an issue of national security.[1] China is undoubtedly one of the world's leading cyber

1. *See, e.g.*, William A. Carter & Daniel G. Sofio, *Cybersecurity Legislation and Critical Infrastructure Vulnerabilities*, *in* FOUNDATIONS OF HOMELAND SECURITY 233, 233 (Martin J. Alperen ed., 2d ed. 2017); Oren Gross, *Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents*, 48 CORNELL INT'L L.J. 481, 481–82 (2015); *see also* DEP'T OF HOMELAND SEC., CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE, at iii (2009),

powers,[2] and its internet policy may have a considerable influence on other jurisdictions.[3] In recent years, China has posed a cyber threat to the United States and many other countries.[4] In the meantime, the country is also facing threats of internet hacking from the United States and other countries.[5] While denying all allegations of initiating cyberattacks,[6] China has endeavored to build its capacity to defend itself against them.[7] The recently enacted Cybersecurity Law[8] not only reflects China's national views on cybersecurity but

---

https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (indicating that "cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century"); Omer Tene, *A New Harm Matrix for Cybersecurity Surveillance*, 12 COLO. TECH. L.J. 391, 398 (2014) ("The vulnerability of . . . [digital] networks and connected infrastructure presents a menacing threat to the functioning of society.").

2. *See, e.g.*, Jyh-An Lee, *The Red Storm in Uncharted Waters: China and International Cyber Security*, 82 UMKC L. REV. 951, 963 (2014); Jyh-An Lee & Ching-Yi Liu, *Real-Name Registration Rules and the Fading Anonymity in China*, 25 WASH. INT'L L.J. 1, 30 (2016); Scott J. Shackelford et al., *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 25 (2016).

3. *See, e.g.*, Jyh-An Lee et al., *Searching for Internet Freedom in China: A Case Study on Google's China Experience*, 31 CARDOZO ARTS & ENT. L.J. 405, 429–30 (2013); *see also* Lee & Liu, *supra* note 2, at 32–33 (analyzing the "spill over" effect of China's internet regulation of real-name registration).

4. *See, e.g.*, Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 404–05 (2007); Wayne Harrop & Ashley Matteson, *Cyber Resilience: A Review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK and USA*, *in* CURRENT AND EMERGING TRENDS IN CYBER OPERATIONS: POLICY, STRATEGY, AND PRACTICE 149, 155–56 (Frederic Lemieux ed., 2015); Lee, *supra* note 2, at 952, 954; Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor,"* 18 VA. J.L. & TECH. 289, 303–04 (2014); *see also* Amitai Etzioni, *The Private Sector: A Reluctant Partner in Cybersecurity*, 15 GEO. J. INT'L AFF. 69, 70 (2014) (describing the huge economic losses suffered by U.S. companies attributable to Chinese hackers).

5. *See, e.g.*, Mirren Gidda, *China's New Cybersecurity Law Could Cost Foreign Companies Their Ideas*, NEWSWEEK (May 31, 2017, 11:35 AM), http://www.newsweek.com/china-cybersecurity-hacking-intellectual-property-multinationals-618345 (reporting that, according to Edward Snowden, as of June 2013 the U.S. "National Security Agency . . . had carried out 61,000 global hacking operations, including in . . . China").

6. *See, e.g.*, Lee, *supra* note 2, at 956.

7. *See, e.g.*, P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 140 (2014) ("China has increasingly taken the position that it must also equip itself for future cyber threats and conflicts."); *see also China's New Cybersecurity Law Sparks Fresh Censorship and Espionage Fears*, GUARDIAN (Nov. 7, 2016, 1:33 AM), https://www.theguardian.com/world/2016/nov/07/chinas-new-cybersecurity-law-sparks-fresh-censorship-and-espionage-fears (citing a National People's Congress official as stating that "China is an internet power, and as one of the countries that faces the greatest internet security risks, urgently needs to establish and perfect network security legal systems").

8. Zhonghua Renmin Gongheguo Wanglao Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law] (promulgated by the Standing Comm. Nat'l People's

also signals the country's determination to build a robust information system that is impervious to cyber threats. Such developments echo Chinese President Xi Jinping's dictum that "without cybersecurity there is no national security."[9]

The Standing Committee of China's National People's Congress ("NPC") passed the Cybersecurity Law on November 7, 2016, and it came into effect on June 1, 2017.[10] This legislation is the first comprehensive law at the national level to address cybersecurity issues.[11] With this new law, the nation-state will have more power to monitor the risks and threats associated with cybersecurity. Although the Chinese government claims that the law is similar to that of other countries,[12] most commentators believe that it is, comparatively, quite unique.[13] Seeking comments, the NPC released a first draft of the law in July 2015 and a second draft in June 2016.[14] Consequently, more than forty business groups petitioned Premier Li Keqiang in August 2016, urging the government to revise some controversial sections found in the second draft.[15] However, the final Cybersecurity Law has been criticized for not adopting any of the substantial comments and criticisms made by private-sector actors—especially foreign businesses—on previous drafts.[16] In May 2017, an

---

Cong., Nov. 7, 2016, effective June 1, 2017), http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm [hereinafter Cybersecurity Law].

9. Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, LAWFARE (June 1, 2017, 10:56 AM), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

10. *See generally* Cybersecurity Law, *supra* note 8.

11. Chiang Ling Li et al., *China's New Cybersecurity Law and Draft Data Localization Measures Expected to Burden Multinational Companies*, JONES DAY (May 2017), http://www.jonesday.com/chinas-new-cybersecurity-law-and-draft-data-localization-measures-expected-to-burden-multinational-companies-05-08-2017/; Carly Ramsey & Ben Wootliff, *China's Cyber Security Law: The Impossibility of Compliance?*, FORBES (May 29, 2017, 3:29 AM), https://www.forbes.com/sites/riskmap/2017/05/29/chinas-cyber-security-law-the-impossibility-of-compliance/.

12. *China's New Cyber Security Laws Will 'Lock Out' Businesses*, ITNEWS (Nov. 8, 2016, 11:57 AM), https://www.itnews.com.au/news/chinas-new-cyber-security-laws-will-lock-out-businesses-440929.

13. Ramsey & Wootliff, *supra* note 11.

14. Ron Cheng, *China Passes Long-Awaited Cyber Security Law*, FORBES (Nov. 8, 2016, 7:07 PM), https://www.forbes.com/sites/roncheng/2016/11/09/china-passes-long-awaited-cyber-security-law/#5924ea3f24d2.

15. *See, e.g.*, Charles Clover & 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; *China's New Cyber Security Laws Will 'Lock Out' Businesses*, *supra* note 12; *China's New Cybersecurity Law Sparks Fresh Censorship and Espionage Fears*, *supra* note 7.

16. *See, e.g.*, Clover & Ju, *supra* note 15; Paul Merrion, *In the Name of Cybersecurity*, CONG. Q. ROLL CALL, Nov. 7, 2016, 2016 WL 6572677 (quoting a Human Rights Watch official as stating that, "[d]espite widespread international concern from corporations and rights advocates for more than a year, Chinese authorities pressed ahead with this restrictive law without making meaningful changes").

alliance of business lobbying groups consisting of American, Asian, and European companies urged the government to delay the implementation of the law,[17] but the Cyberspace Administration of China ("CAC") only agreed to delay the execution of regulations governing cross-border data flow until the end of 2018.[18] In June 2017, the Computer and Communications Industry Organization ("CCIO")—a major industry organization in the United States representing firms such as Amazon, Microsoft, Mozilla, and Intel—urged the Trump administration to pressure China to back off the law.[19]

Foreign businesses' criticism of China's Cybersecurity Law mostly focuses on the policy goals behind the law and the vague language used therein.[20] For example, James Zimmerman, then-chairman of the American Chamber of Commerce in China, described the law as "a step backwards for innovation in China that won't do

---

17. Sui-Lee Wee, *China's New Cybersecurity Law Leaves Foreign Firms Guessing*, N.Y. TIMES (May 31, 2017), https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html?mcubz=0; *see also China to Launch Cybersecurity Law Despite Concerns*, EXPRESS TRIB. (May 30, 2017), https://tribune.com.pk/story/1422794/china-launch-cybersecurity-law-despite-concerns/ (reporting that "[t]he European Union Chamber of Commerce, among other groups, has urged Beijing to 'delay the implementation of either the law or its relevant articles'").

18. Wee, *supra* note 17.

19. Paul Merrion, *Leading Tech Firms Urge White House to Fight China's New Cyber Law*, CONG. Q. ROLL CALL, June 6, 2017, 2017 WL 2437176.

20. *See, e.g.*, Emilio Iasiello, *China's Cyber Initiatives Counter International Pressure*, 10 J. STRATEGIC SECURITY 1, 8 (2017) ("Creating the most uneasiness is the vagueness surrounding the language of the law."); Nick Akerman et al., *China Adopts Tough and Sweeping Cybersecurity Law*, THETMCA.COM (Dec. 7, 2016), https://thetmca.com/china-adopts-tough-and-sweeping-cybersecurity-law/ ("The law is broadly drafted, filled with ambiguities and creates significant potential uncertainties for companies doing business in China . . . ."); *China to Launch Cybersecurity Law Despite Concerns*, *supra* note 17 (quoting Jacob Parker, vice president of the US-China Business Council, as asserting that "[i]t's been enormously difficult for our companies to prepare for the implementation of the cybersecurity law, because there are so many aspects of the law that are still unclear"); *China's Cyber Security Law and its Chilling Effects*, FIN. TIMES (June 2, 2017), https://www.ft.com/content/60913b9e-46b9-11e7-8519-9f94ee97d996; Li et al., *supra* note 11 ("The . . . new law has been widely criticized as containing a number of broadly defined terms and vague provisions that potentially—and significantly—affect a wide range of companies."); Ross O'Brien & John Gruetzner, *Cyber Law Creates Hurdle to Chinese Internet Companies' Growth*, NIKKEI ASIAN REV. (June 16, 2017, 6:00 PM), https://asia.nikkei.com/Viewpoints/Ross-O-Brien-and-John-Gruetzner/Cyber-law-creates-hurdle-to-Chinese-internet-companies-growth (reporting that "[t]he law has been widely criticized for its ambiguity"); Sacks, *supra* note 9 ("[T]he language of the law is broad and ambiguous, and that vagueness creates problematic uncertainties."); Xiaoyan Zhang, *Cracking China's Cybersecurity Law*, CHINA L. & PRAC. (Jan. 19, 2017), http://www.chinalawandpractice.com/sites/clp/2017/01/19/cracking-chinas-cybersecurity-law/ ("Further muddying the waters are looming uncertainties implicit in the law, including ambiguities in language and several critical terms . . . .").

much to improve security"[21] and argued that it is too "vague, ambiguous, and subject to broad interpretation by regulatory authorities."[22] Michael Chang, vice president of the European Union Chamber of Commerce, also complained that the law is too ambiguous and confusing.[23] The uncertainties surrounding the law could stop foreign companies from bringing their best technologies to China.[24] The vagueness and ambiguity underlying the law may enable the government to enforce it in an opaque and discriminatory way.[25] Some commentators have suggested that such ambiguities were created intentionally so that the Communist Party could have leeway to target internet companies.[26] Others claimed that the law would be used to protect domestic products against foreign competition[27] and that it emphasizes "protectionism [more] than security."[28] Undoubtedly, the law has imposed greater state control over businesses and internet users.[29] As a result, it is not surprising that

---

21. Andrew Blake, *Chinese Cyber Law Challenged by Tech Titans Over Intellectual Property, Security Concerns: Report*, WASH. TIMES (Dec. 2, 2016), http://www.washingtontimes.com/news/2016/dec/2/chinese-cyber-law-challenged-tech-titans-over-inte/.

22. *China's New Cybersecurity Law Sparks Fresh Censorship and Espionage Fears*, *supra* note 7; *see also* Gidda, *supra* note 5 ("Wide-ranging and loosely worded, [the Cybersecurity Law] is likely to make life much harder for foreign companies who do business in China."). For the exact vague language in the law, see, for example, *infra* text accompanying notes 90, 123–28, 139–40, 197–98.

23. Wee, *supra* note 17.

24. *Id.*; *see also* Ramsey & Wootliff, *supra* note 11 ("[D]eciphering exactly ***who*** is captured and ***what*** is covered is leaving companies unsure as to how they will comply with this vague and potentially onerous law.").

25. *See e.g.*, *China to Launch Cybersecurity Law Despite Concerns*, *supra* note 17 (reporting that the European Union Chamber of Commerce "called on policymakers to follow a 'transparent' process that will help eliminate 'discriminatory market access barriers'").

26. Wee, *supra* note 17.

27. *See, e.g.*, Iasiello, *supra* note 20, at 1; *China Adopts a Tough Cyber-Security Law*, ECONOMIST (Nov. 10, 2016), https://www.economist.com/news/china/21710001-foreign-firms-are-worried-china-adopts-tough-cyber-security-law; *China to Launch Cybersecurity Law Despite Concerns*, *supra* note 17; Clover & Ju, *supra* note 15; Georges Haour, *Why China's New Cybersecurity Law Is Bad News for Business*, FORTUNE (Dec. 1, 2016), http://fortune.com/2016/12/01/china-cybersecurity-law-business/; Lotus Ruan, *What Does China's New Cybersecurity Law Mean for Chinese Internet Companies?*, DIPLOMAT (Nov. 10, 2016), http://thediplomat.com/2016/11/what-does-chinas-new-cybersecurity-law-mean-for-chinese-internet-companies/.

28. Clover & Ju, *supra* note 15; *see also* Josh Chin & Eva Dou, *China's New Cybersecurity Law Rattles Foreign Tech Firms*, WALL ST. J. (Nov. 7, 2016, 3:38 AM), https://www.wsj.com/articles/china-approves-cybersecurity-law-1478491064 (reporting that foreign companies feel that the policies underlying the Cybersecurity Law "cite national security for protectionist purposes"); Merrion, *supra* note 19 (describing the CCIO's viewpoint that the Cybersecurity Law "effectively is protectionism disguised as cybersecurity and data privacy measures").

29. *See, e.g.*, *China's Cyber Security Law and its Chilling Effects*, *supra* note 20; *China's New Cybersecurity Law Sparks Fresh Censorship and Espionage*

some suspect that China is enforcing its censorship policy under the guise of cybersecurity.[30]

This Article provides a thorough analysis of key provisions in China's Cybersecurity Law, including their functions, limitations, and relevant policy implications. Part II introduces the background of the Cybersecurity Law, demonstrating how the law has institutionalized China's longstanding assertion of internet sovereignty under the pretense of protecting cybersecurity. Moreover, Part II will discuss how the Cybersecurity Law is not a piece of standalone legislation but instead should be viewed as part of the nation-state's legislative endeavors to strengthen national security. Together with the Great Firewall, the National Security Law, the Counterterrorism Law, and other internet regulations, the Cybersecurity Law has been crafted as an indispensable foundation for China's authoritarian control over the internet. Part III then identifies the major legal issues found within the Cybersecurity Law, which include the obligation of network operators, the defense of critical infrastructure, data localization, security review, and the protection of personal information. Part IV examines the policy implications and characteristics of the Cybersecurity Law by showing how the law reflects China's unique approaches to cybersecurity and human rights, which are significantly different from the approaches taken in the Western world. Further, Part IV will reveal that the law also represents the government's distrust of the market when it comes to cybersecurity issues and how the overly broad language used in the law remains an unresolved issue for both regulators and industry. Finally, Part V concludes this Article.

II. BACKGROUND AND FOUNDATION OF THE CYBERSECURITY LAW

The Cybersecurity Law does not exist in a vacuum. The law is a milestone in a series of policy initiatives and legislation aimed at strengthening the protection of national security and cybersecurity in China in recent years. Therefore, this legislation should be understood alongside other laws—such as the National Security Law and the Counterterrorism Law—and China's unique internet architecture. Moreover, the design of the Cybersecurity Law was based on the concept of "cyberspace sovereignty" that shapes China's overall internet policy and regulations.[31]

Fears, *supra* note 7; Arya MM, *Will China's Cyber Security Law Restrict Online Freedom?*, INFOTECHLEAD (Nov. 7, 2016), http://www.infotechlead.com/security/will-chinas-cyber-security-law-restrict-online-freedom-43755.

30. *See, e.g.*, Iasiello, *supra* note 20, at 7; Shackelford et al., *supra* note 2, at 30.

31. Iasiello, *supra* note 20, at 3.

A. Background of the Cybersecurity Law

The United States has identified China as probably the most important digital power in the world in terms of creating national security concerns.[32] Both the U.S. government and American businesses have been exposed to Chinese hacking of confidential information.[33] Nonetheless, the intelligence leaks from Edward Snowden have shown that the United States has similarly engaged in internet surveillance of multiple nations around the world, including China.[34] Obviously, China has also had to cope with national security problems caused by various actions of foreign governments via their intelligence agents.[35] Unsurprisingly, China claims that it has been a victim of hack attacks.[36] The U.S. intelligence activities disclosed by Snowden are likely a small part of a much bigger threat against China's national security. Furthermore, the rapid development of digital technologies in China and the interconnected nature of the internet have also made cybersecurity a national priority for the country.[37] President Xi Jinping has therefore emphasized that security is a prerequisite for internet development.[38] As a result, in February 2014, the Chinese Communist Party announced the creation of the Cybersecurity and Informatization Leading Group, chaired by President Xi Jinping, in order to address cybersecurity issues.[39] The establishment of this group represents

---

32. *See* Eric Blinderman & Myra Din, *Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime*, 50 VAND. J. TRANSNAT'L L. 889, 896–97 (2017); Jyh-An Lee, *The Sino-US Digital Relationship and International Cyber Security*, *in* CURRENT AND EMERGING TRENDS IN CYBER OPERATIONS: POLICY, STRATEGY, AND PRACTICE, *supra* note 4, at 84, 84–88; Jon R. Lindsay, *The Impact of China on Cybersecurity*, 39 INT'L SECURITY 7, 7 (2015).

33. *See, e.g.*, Blinderman & Din, *supra* note 32, at 895–97; Scott J. Shackelford et al., *Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector*, *in* ETHICS AND POLICIES FOR CYBER OPERATIONS 115, 128 (Mariarosaria Taddeo & Ludovica Glorioso eds., 2017); Lindsay, *supra* note 32, at 7, 26–27.

34. *See, e.g.*, Lindsay, *supra* note 32, at 7–8; Tatevik Sargsyan, *Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security*, 10 INT'L J. COMM. 2221, 2225–26 (2016).

35. John Selby, *Data Localization Laws: Trade Barrier or Legitimate Responses to Cybersecurity Risks, or Both?*, 25 INT'L J.L. & INFO. TECH. 213, 231 (2017).

36. *See, e.g.*, Lee, *supra* note 2, at 957–58; Chin & Dou, *supra* note 28.

37. *See, e.g.*, Iasiello, *supra* note 20, at 1–3.

38. Tian Shaohui, *China's Xi Calls for Better Development of Internet*, XINHUA NEWS (Apr. 19, 2016), http://news.xinhuanet.com/english/2016-04/19/c_135294307.htm; *see also* Shackelford et al., *supra* note 33, at 129 (documenting President Xi Jinping's statement that "a uniform and comprehensive approach to 'network security' is necessary to turn China into a 'cyber power'").

39. *See, e.g.*, KPMG, OVERVIEW OF CHINA'S CYBERSECURITY LAW 4 (2017), https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf; *see also* Iasiello, *supra* note 20, at 3–5 (noting that the establishment of this group represents the government's key initiative associated

the President and Premier's direct involvement in cybersecurity policy, which has been elevated to a national concern.[40] Prior to the enactment of the Cybersecurity Law, China had issued some administrative measures and rules associated with cybersecurity, such as the Regulations on Security Protection of Computer Information Systems, the Administrative Measures for Prevention and Treatment of Computer Viruses, and the Administrative Measures for Hierarchical Protection of Information Security.[41] China has also endeavored to enhance its cybersecurity by collaborating with the United States. Recently, U.S. President Donald Trump and Chinese President Xi Jinping agreed to establish a high-level dialogue mechanism on cybersecurity when they met in Florida in April 2017,[42] and the conversation between the two governments is ongoing.[43]

China has viewed cybersecurity as a national security issue[44] and the Cybersecurity Law bears witness to the Chinese government's continuous legislative effort to strengthen its national security. The recent legislative wave regarding national security in China started with the National Security Law, promulgated on July 1, 2015,[45] which provides the government with broad authority to implement a system for cybersecurity. Concerns have been raised by critics that the law may be used to crack down on peaceful expression.[46] While the main function of the National Security Law is to provide a legal framework to respond to emerging threats to national security,[47] it is similar to the Cybersecurity Law in that both laws have empowered the government to monitor and control the flow of information and have increased scrutiny of foreign technologies.[48] Furthermore, both laws stress the concept of cyberspace sovereignty, which China has

---

with cybersecurity); Lindsay, *supra* note 32, at 17; Stephen Chen, *Xi Jinping Heads New Panel on Internet Security and Promoting IT*, SOUTH CHINA MORNING POST (Feb. 28, 2014, 4:57 AM), http://www.scmp.com/news/china/article/1436747/xi-jinping-heads-new-panel-internet-security-and-promoting-it; MM, *supra* note 29 (stating that, "[s]ince Edward Snowden's revelations about U.S. spying, China has become more aggressive about its cyber security").

40. *See, e.g.*, Iasiello, *supra* note 20, at 6.

41. KPMG, *supra* note 39.

42. An Baijie, *Xi's Guidance Focuses Push on Internet*, CHINA DAILY (Apr. 20, 2017), http://www.chinadaily.com.cn/china/2017-04/20/content_29003244.htm.

43. *See, e.g.*, Iasiello, *supra* note 20, at 3.

44. *Id.* at 2; Ruan, *supra* note 27; *see also* Chen, *supra* note 39 (reporting President Xi Jinping's statement that "[t]here is no national security without internet security").

45. Zhonghua Renmin Gongheguo Guojia Anquan Fa (中华人民共和国国家安全法) [National Security Law] (promulgated by Standing Comm. Nat'l People's Cong., July 1, 2015, effective July 1, 2015), http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm [hereinafter National Security Law].

46. Margaret K. Lewis, *Human Rights and the U.S.-China Relationship*, 49 GEO. WASH. INT'L L. REV. 471, 490–91 (2017).

47. Iasiello, *supra* note 20, at 9.

48. *Id.* at 7–8.

actively claimed.[49] Some commentators believe that both laws represent a series of efforts "to secure the regime and its power."[50]

After the enactment of the National Security Law, the NPC passed the Counterterrorism Law on December 27, 2015, and the law came into effect on January 1, 2016.[51] The Counterterrorism Law includes a few provisions associated with cybersecurity issues, as it requires telecommunications business operators and internet service providers ("ISPs") to provide technical support and assistance—such as technical interface and decryption—to public security authorities and national security authorities for the purposes of preventing and investigating terrorist activities.[52] Telecommunications business operators and ISPs are further obliged to protect cybersecurity and implement content supervision rules and technical measures for security protection so as to prevent the dissemination of information containing terrorist or extremist content.[53] The law also grants competent authorities the legal power to order applicable entities to cease the transmission of and delete relevant information pertaining to any terrorist or extremist content as well as to order such entities to shut down the relevant websites and terminate the provision of the relevant services.[54] Competent telecommunications authorities are also required to block terrorist or extremist content transmitted from abroad via the internet.[55] The Chinese government previously planned to require data localization in the Counterterrorism Law but removed the provision from its final draft in December 2015.[56] The provision eventually became Article 37 of the Cybersecurity Law.[57] Overall, the Counterterrorism Law has facilitated technology compliance and government control and monitoring of information in the name of security.[58]

49. *See infra* text accompanying note 69.

50. Ruan, *supra* note 27.

51. Zhonghua Renmin Gongheguo Fan Kongbu Zhuyi Fa (中华人民共和国反恐怖主义法) [Counterterrorism Law] (promulgated by Standing Comm. Nat'l People's Cong., Dec. 27, 2015, effective Jan. 1, 2016), http://www.npc.gov.cn/npc/xinwen/2015-12/28/content_1957401.htm.

52. *Id.* art. 18.

53. *Id.* art. 19.1.

54. *Id.* art. 19.2.

55. *Id.*

56. Sacks, *supra* note 9.

57. *Id.*

58. Iasiello, *supra* note 20, at 11.

B. Cyberspace Sovereignty

Cyberspace sovereignty, sometimes referred to as "internet sovereignty,"[59] "network sovereignty,"[60] or "cyber sovereignty,"[61] has become a fundamental principle in China's Cybersecurity Law and other internet-related policies.[62] Article 1 of the Cybersecurity Law makes clear that the law's legislative purpose is "to protect cybersecurity; to safeguard cyberspace sovereignty, national security, and the societal public interest; to protect the lawful rights and interests of citizens, legal persons, and other organizations; and to promote the healthy development of economic and social informatization."[63] The law unequivocally approaches cybersecurity concerns as a threat to sovereignty and national security.[64]

Conventional wisdom dictates that there are no borders in cyberspace;[65] therefore, there should be no sovereignty in cyberspace. Nonetheless, Article 1 of the law clearly claims that one of its main purposes is to "safeguard cyberspace sovereignty."[66] In fact, the Cybersecurity Law is not the first Chinese law or government statement claiming the nation's cyberspace sovereignty. The Chinese State Council Information Office released a white paper entitled "The Internet in China" in 2010 outlining China's internet policy,[67] which was the first document of its kind. The white paper drew a link

---

59. *See, e.g.*, Min Jiang, *Authoritarian Informationalism: China's Approach to Internet Sovereignty*, 30 SAIS REV. INT'L AFF. 71, 72 (2010); Shackelford et al., *supra* note 2, at 31.

60. Max Parasol, *The Impact of China's 2016 Cyber Security Law on Foreign Technology Firms, and on China's Big Data and Smart City Dreams*, 34 COMPUTER L. & SECURITY REV. 67, 72–73, 75 (2018).

61. *See, e.g.*, SUSAN PERRY & CLAUDIA RODA, HUMAN RIGHTS AND DIGITAL TECHNOLOGY: DIGITAL TIGHTROPE 106 (2017); Zhixiong Huang & Kubo Mačák, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, 16 CHINESE J. INT'L L. 271, 292–96 (2017); Shackelford et al., *supra* note 2, at 1; Samson Yuen, *Becoming a Cyber Power: China's Cybersecurity Upgrade and Its Consequence*, 2015 CHINA PERSP. 53, 54 (2015).

62. *See, e.g.*, Cybersecurity Law, *supra* note 8, art. 1; Yuen, *supra* note 61; *see also* Scott J. Shackelford et al., *iGovernance: The Future of Multi-Stakeholder Internet Governance in the Wake of the Apple Encryption Saga*, 42 N.C. J. INT'L L. 883, 917 (2017) (noting that China has promoted "cybersecurity as a subset of national sovereignty"); Shackelford et al., *supra* note 2, at 31 ("China's take on cybersecurity is reflected in the idea of Internet sovereignty.").

63. Cybersecurity Law, *supra* note 8, art. 1.

64. *Cf.* Condron, *supra* note 4, at 407 (stating that the United States used to operate "under the presumption that a cyber attack constitutes a criminal activity, not a threat to national security").

65. *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 25–27 (2006); Condron, *supra* note 4, at 409; David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996).

66. Cybersecurity Law, *supra* note 8, art. 1.

67. INFO. OFFICE OF THE STATE COUNCIL OF CHINA, INTERNET IN CHINA 2 (2010), http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN042565.pdf.

between cyberspace sovereignty and cybersecurity, or "internet security," by proclaiming that

> within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security.[68]

The National Security Law enacted in 2015 further stressed that the state should "maintain cyberspace sovereignty" by "strengthening network management [and] preventing, stopping, and lawfully punishing illegal and criminal internet activities, including cyberattacks, network hacking, cybertheft, and dissemination of unlawful and harmful information."[69]

Whether nation-states possess sovereignty over cyberspace is debatable. Nonetheless, a nation-state certainly possesses sovereignty over both its domestic network[70] and the cyber infrastructure located within its territory.[71] Governments can thus put the idea of cyberspace sovereignty into practice by leveraging internet infrastructure configurations within their territories. Therefore, from a regulatory perspective, the internet and its governance are far from borderless.[72] This outlook is exactly how China's Cybersecurity Law regulates cyberspace, as a significant part of the law concerns the regulation of domestic internet operators and critical infrastructure.[73] In fact, China has built borders for cyberspace within its internet architecture—i.e., the Great Firewall—which has effectively facilitated the filtering and blocking of foreign online content.[74] President Xi Jinping and the Chinese government

---

68. *Id.* at 13–15.

69. National Security Law, *supra* note 45, art. 25.

70. *See, e.g.*, Shackelford et al., *supra* note 2, at 11–12.

71. *See, e.g.*, GOLDSMITH & WU, *supra* note 65, at 68–74, 93–97; Gross, *supra* note 1, at 499.

72. *See, e.g.*, Jiang, *supra* note 59, at 74.

73. *See, e.g.*, Shackelford et al., *supra* note 2, at 30–31.

74. *See, e.g.*, ANUPAM CHANDER, THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD TOGETHER IN COMMERCE 193–201 (2013); REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM 35 (2012); PERRY & RODA, *supra* note 61, at 99–104; Jiang, *supra* note 59, at 75; Lee et al., *supra* note 3, at 424–26; Lindsay, *supra* note 32, at 15; Yuen, *supra* note 61, at 53; Clover & Ju, *supra* note 15; *see also* Jyh-An Lee & Ching-Yi Liu, *Forbidden City Enclosed by the Great Firewall*, 13 MINN. J.L. SCI. & TECH. 125, 151 (2012) (stating that the filtering systems disable the internet's power to eliminate sovereignty); Uchenna Jerome Orji, *An Analysis of China's Regulatory Response to Cybersecurity*, 18 COMPUTER & TELCOMM. L. REV. 212, 212 (2012) (indicating that the Great Firewall is an important part of China's

have used the term "cyberspace sovereignty" to indicate that nation-states can choose to develop and regulate their internet environments as they like within their borders,[75] and cyberspace sovereignty has become a fundamental philosophy underlying China's internet policy.[76] In the physical world, China has used the term "sovereignty" to defend its human rights record from external criticism.[77] As numerous internet regulations aim to restrict certain fundamental human rights, such as free speech and privacy,[78] it is not surprising that China has extended its sovereignty to include cyberspace in order to obviate foreign interference. The Cybersecurity Law reaffirms China's claim over cyberspace sovereignty,[79] examples of which include the strict data localization requirement and other strict regulations in the law.[80] Therefore, some Western observers argue

---

cybersecurity policy); Shackelford et al., *supra* note 62, at 916 (noting that the Great Firewall is an example of China's claim over internet sovereignty).

75. *See, e.g.*, Huang & Mačák, *supra* note 61, at 293; Iasiello, *supra* note 20, at 1; Jiang, *supra* note 59, at 72–73; Yuen, *supra* note 61; *China Internet: Xi Jinping Calls for "Cyber Sovereignty,"* BBC NEWS (Dec. 16, 2015), http://www.bbc.com/news/world-asia-china-35109453; Zolzaya Erdenebileg, *China's New Cybersecurity Law to be Implemented on June 1*, CHINA BRIEFING NEWS (Mar. 16, 2017), http://www.china-briefing.com/news/2017/03/16/china-new-cybersecurity-law-to-be-implemented-june-1.html; *see also* Shackelford et al., *supra* note 33 (describing China's attempt to shape international norms regarding "the sovereign state's control over domestic Internet").

76. *See, e.g.*, Yuen, *supra* note 61.

77. *See, e.g.*, Dongsheng Zhang, *China's "Attitude" Toward Human Rights: Reading Hungdah Chiu in the Era of the Iraq War*, 27 MD. J. INT'L L. 263, 265 (2012); *see also* Daniel C.K. Chow, *How China Uses International Trade to Promote Its View of Human Rights*, GEO. WASH. INT'L L. REV. 681, 683 (2013) (noting China's viewpoint that human rights are derived from a fundamentally different vision of national sovereignty than that of the Western world); Randall Peerenboom, *Assessing Human Rights in China: Why the Double Standard?*, 38 CORNELL INT'L L.J. 71, 73 (2005) (stating that Chinese citizens view foreign criticisms of China's human rights status as infringing on the country's sovereignty).

78. *See, e.g.*, Cybersecurity Law, *supra* note 8, art. 24 (requiring network operators to obtain a user's true identity before providing them with services).

79. *See, e.g.*, Iasiello, *supra* note 20, at 7 (citing a Chinese media report indicating that the Cybersecurity Law "safeguards sovereignty on cyberspace"); *id.* at 14 ("By . . . implementing cybersecurity in all of its legislation, China is legally guaranteeing its rights as a cyber sovereign."); Ruan, *supra* note 27 (quoting Yang Heqing, spokesman for the NPC Legislative Affairs Commission, as noting that the law reinstated "China's long-advocated concept of Internet sovereignty"); *see also* John Leyden, *China Cyber-Security Law Will Keep Citizens' Data Within the Great Firewall*, REGISTER (June 1, 2017, 11:31 AM), https://www.theregister.co.uk/2017/06/01/china_cybersecurity_law/ (citing Bill Hagestad, an expert in cybersecurity, as being of the opinion that the law "is designed to protect the cyber borders of China against foreign negative influences").

80. *See infra* Subpart III.C; *see also* Alexander Savelyev, *Russia's New Personal Data Localization Regulations: A Step Forward or A Self-Imposed Sanction?*, 32 COMPUTER L. & SECURITY REV. 128, 140 (2016) (noting that Russia's data localization law is based on the concept of "digital sovereignty").

that China uses this term in order to "legitimize authoritarian control" over cyberspace.[81]

III. MAIN LEGAL ISSUES

In addition to institutionalizing some longstanding internet policies and government practices in China,[82] the Cybersecurity Law also establishes certain national mechanisms to protect cybersecurity. This Part examines key legal issues in the Cybersecurity Law, which include the legal obligations of network operators, the defense of critical infrastructure, the data localization requirement, security inspection and review, and the protection of personal information.

A. Network Operators

Intermediaries, such as ISPs, search engines, and social media outlets, have been targeted by nation-states to enforce their internet regulations.[83] The Cybersecurity Law continues China's current practice of implementing internet regulations on intermediaries.[84] Intermediaries, especially ISPs, play an important role in censoring and blocking unwanted foreign websites.[85] Unsurprisingly, the Cybersecurity Law also imposes significant obligations on intermediaries—namely, network operators, critical information infrastructure operators, and suppliers of network products and services.[86]

---

81. Lindsay, *supra* note 32, at 13; *see also* Parasol, *supra* note 60, at 75 (explaining that "China's conception of Network Sovereignty is that the internet is subject to national boundaries that individual countries should control").

82. *See, e.g.*, Chin & Dou, *supra* note 28; *China's New Cyber Security Laws Will 'Lock Out' Businesses*, *supra* note 12; *China's New Cybersecurity Law Sparks Fresh Censorship and Espionage Fears*, *supra* note 7; Paul Mozur, *China's Internet Controls Will Get Stricter, to Dismay of Foreign Business*, N.Y. TIMES (Nov. 7, 2016), https://www.nytimes.com/2016/11/08/business/international/china-cyber-security-regulations.html; *see also* Ramsey & Wootliff, *supra* note 11 ("The new [Cybersecurity Law] . . . to some extent consolidates cyber activities captured in other laws and regulations."); Ruan, *supra* note 27 (citing Zhang Lifan, a Chinese historian, as noting that—with regard to the Cybersecurity Law—"[m]any of the measures are in place already"); Sara Xia, *China Cybersecurity and Data Protection Laws: Chang Is Coming*, CHINA L. BLOG (May 10, 2017), http://www.chinalawblog.com/2017/05/china-cybersecurity-and-data-protection-laws-change-is-coming.html (stating that "China's new Cybersecurity Law adopts and modifies existing regulations and codifies them").

83. *See, e.g.*, GOLDSMITH & WU, *supra* note 65, at 69–72; Sargsyan, *supra* note 34, at 2221–22, 2224.

84. *See, e.g.*, Lee & Liu, *supra* note 74, at 148–49.

85. *See, e.g.*, *id.* at 148–50; Lindsay, *supra* note 32, at 15.

86. *See, e.g.*, Cybersecurity Law, *supra* note 8, art. 25 (requiring network operators to develop emergency plans for handling network security incidents and responding to security risks, such as system vulnerabilities, viruses, or cyberattacks, and to report any such event to the relevant authorities); *id.* art. 38 (demanding that critical information infrastructure operators evaluate and

The law defines "network operators" as "network owners, managers, and Internet service providers."[87] This definition has been criticized for its breadth[88] because it can include anyone operating a business over the internet.[89] Some commentators suspect that the government has purposely defined "network operator" broadly in the law to provide a wider scope for future interpretations.[90] Network operators' primary obligations under Article 21 are to (1) formulate internal security management systems and operating rules, determine personnel responsible for network security, and implement network security protection responsibilities; (2) adopt technological measures to prevent computer viruses, network attacks, network intrusions, and other actions endangering network security; (3) adopt technological measures for monitoring and recording network operational statuses and network security incidents and follow relevant provisions to store network logs for at least six months; and (4) adopt measures such as data classification, back-ups of important data, and encryption, along with other obligations provided by law or administrative regulations.[91] Moreover, the law requires network operators to develop emergency response plans to react to cybersecurity incidents, and, in the event of an incident, operators are obliged to promptly implement remediation measures and report the incident to the relevant authorities.[92] If network operators fail to fulfill any of these obligations, the competent authorities will order corrections and give warnings.[93] Where corrections are refused or lead to the endangerment of network security or other such consequences, a fine of between RMB 10,000 and 100,000 (approximately $1,590 and $15,920, respectively) will be imposed, and management personnel directly responsible will be personally

---

improve detection measures); *id.* art. 22 (mandating that network products and services comply with national standards, prohibiting the operation of malicious programs, and requiring product and service providers to immediately report security flaws or vulnerabilities to users and relevant authorities and take remedial action).

87. *Id.* art. 76.

88. Cheng, *supra* note 14.

89. *See, e.g.*, Bret Cohen et al., *Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy*, ANTITRUST, Fall 2017, at 107, 109; Donfil Huang & Olivier Maugain, *New China Cybersecurity Law Impacts Use of "Personal Information,"* CAMPAIGN ASIA (May 31, 2017), http://www.campaignasia.com/article/new-china-cybersecurity-law-impacts-use-of-personal-information/436722; Katherine W. Keally, *China's Cybersecurity Law Goes Into Effect June 1, 2017—Are You Ready?*, NAT'L ASS'N CORP. DIRECTORS (Mar. 21, 2017), https://blog.nacdonline.org/2017/03/chinas-cybersecurity-law-goes-into-effect-june-1-2017-are-you-ready/; Li et al., *supra* note 11.

90. Xia, *supra* note 82.

91. Cybersecurity Law, *supra* note 8, art. 21.

92. *Id.* art. 25.

93. *Id.* art. 59.

fined between RMB 5,000 and 50,000 (approximately $800 and $7,960, respectively).[94]

Article 24 requires network operators to implement the real-name registration scheme for their consumers using services associated with network access, domain registration, landline or mobile phone network access, information publication, and instant messaging.[95] Further, the law prohibits network operators from providing services to users who do not provide their true identity.[96] If network operators fail to require users to provide real identity information or deliver relevant services to users who do not provide real identity information, the relevant authorities will order corrections.[97] If network operators refuse to make corrections or the circumstances are particularly serious, they will be fined between RMB 50,000 and 500,000 (approximately $7,960 and $79,620, respectively), and the relevant competent department may order a temporary suspension of operations, close down websites, cancel relevant operations permits, or cancel business licenses.[98] Persons who are directly in charge and other directly responsible personnel will be fined between RMB 10,000 and 100,000 for such infractions (approximately $1,590 and $15,920, respectively).[99]

Network operators are also required by Article 28 to provide technical support and assistance to public security agencies in order to preserve national security and investigate crimes.[100] As a result, the regulatory authorities have more monitoring, investigative, and enforcement powers. However, this also means that, by cooperating with government authorities, network operators may expose their data to a higher risk of leakage. Concerns have been raised that government agencies may mandate internet companies to provide access or decryption assistance to obtain users' confidential information[101] even without a warrant, subpoena, or any type of court order.[102] Network operators may arguably be required to create backdoors within their product for the government to access their data accordingly.[103] Similar concerns were raised when China passed the Counterterrorism Law, which likewise requires

94. *Id.* (currency conversions last updated Apr. 1, 2018).
95. *Id.* art. 24.
96. *Id.*
97. *Id.* art. 61.
98. *Id.* (currency conversions last updated Apr. 1, 2018).
99. *Id.* (currency conversions last updated Apr. 1, 2018).
100. *Id.* art. 28.
101. *See, e.g.*, Justin (Gus) Hurwitz, *Encryption^{Congress} Mod (Apple + CALEA)*, 30 HARV. J.L. & TECH. 355, 417 n.267 (2017); Keally, *supra* note 89.
102. Cybersecurity Law, *supra* note 8, art. 28 ("Network operators shall provide technical support and assistance to public security organs and state security agencies in safeguarding their national security and investigating crimes in accordance with the law.").
103. *China's New Cyber Security Laws Will 'Lock Out' Businesses*, *supra* note 12.

telecommunications business operators and ISPs to provide the government with decryption and other technical support for the purposes of preventing and investigating terrorist activities.[104] The Chinese government then claimed that "there is technically no requirement [in the Counterterrorism Law] for companies to install backdoors."[105] These concerns, however, are not unique to China. Internet companies in other jurisdictions may also cooperate with governments to provide decryption assistance or backdoor access to personal data for law enforcement purposes.[106] Unfortunately, the Cybersecurity Law neither limits the government's law enforcement power to only what is strictly necessary nor provides other guidelines concerning under what circumstances government agencies can enforce this provision for the purposes of national security.[107]

B. Critical Infrastructure

"Critical infrastructure" refers to the facilities, systems, and networks that are socially and economically crucial to the functioning of a country in terms of how goods or services provided therein are essential to national security, economic vitality, and citizen health and safety.[108] Critical infrastructure covers a wide variety of sectors, including agriculture, food, water, energy, health, communications, transportation, financial systems, etc.[109] Since critical infrastructure is vital to a nation's survival,[110] then-President Barack Obama declared critical infrastructure to be a "strategic national asset."[111]

---

104. Shackelford et al., *supra* note 62, at 920–21.

105. *Id.* at 921.

106. *See, e.g.*, Sargsyan, *supra* note 34, at 2222; *China's New Cybersecurity Law Sparks Fresh Censorship and Espionage Fears*, *supra* note 7.

107. *Cf.* Kate Conger, *China's New Cybersecurity Law is Bad News for Business*, TECHCRUNCH (Nov. 6, 2016), https://techcrunch.com/2016/11/06/chinas-new-cybersecurity-law-is-bad-news-for-business/.

108. *See, e.g.*, TED G. LEWIS, CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY: DEFENDING A NETWORKED NATION 7–8 (2d ed. 2015) [hereinafter LEWIS, CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY]; JAMES A. LEWIS, CTR. FOR STRATEGIC & INT'L STUDIES, CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION 1, 4 (2006), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf; Harrop & Matteson, *supra* note 4, at 152.

109. *See, e.g.*, LEWIS, CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY, *supra* note 108, at 8; Cristina Alcaraz & Sherali Zeadally, *Critical Infrastructure Protection: Requirements and Challenges for the 21st Century*, 8 INT'L J. CRITICAL INFRASTRUCTURE PROTECTION 53, 53–54 (2015); Condron, *supra* note 4, at 406; Palmer, *supra* note 4, at 294.

110. *See, e.g.*, Condron, *supra* note 4, at 407; Gross, *supra* note 1, at 482.

111. President Barack Obama, Remarks by the President on Securing our Nation's Cyber Infrastructure (May 29, 2009), https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

Because of the centrality of the internet and digital technologies in all aspects of critical infrastructure,[112] such infrastructure is increasingly vulnerable to cyberattacks and other forms of cyber threats.[113] Cyberattacks on critical infrastructure may come from other nation-states that aim to "penetrate networks, collect information, and observe activities without arousing suspicion."[114] Thus, the protection of critical infrastructure has become an important policy issue associated with cybersecurity.[115] Nevertheless, many critical infrastructure assets are in the hands of private companies[116] that may lack the incentives to make significant investments to defend their networks from cyberattacks.[117] Therefore, policymakers always need to explore optimal regulatory approaches to encourage the private sector's investment in cybersecurity.

The protection of critical infrastructure has been an essential element of China's cybersecurity strategy since 2003 and continues to be central to the country's current cybersecurity policy.[118] The Cybersecurity Law further aims to answer one of the most difficult policy questions in terms of protecting critical infrastructure: "[W]ho is responsible for what?"[119] Article 31 of China's Cybersecurity Law elucidates how critical information infrastructure[120] includes, but is not limited to, public communication and information services, energy, transportation, water conservation, banking and finance, public services, and electronic government.[121] The same provision defines "critical information infrastructure" as that which, if

112. *See, e.g.*, William de Laat, *The Beyond the Border Action Plan: A Tool for Enhanced Canada–U.S. Cooperation on Critical Infrastructure and Cyber Security – Or More Window Dressing?*, 37 CAN.–U.S. L.J. 451, 453 (2012).

113. *See, e.g.*, Carter & Sofio, *supra* note 1; Daniela Oliveira, *Cyber-Terrorism and Critical Energy Infrastructure Vulnerability to Cyber-Attacks*, 5 ENVTL. & ENERGY L. & POL'Y J. 519, 520 (2010); *see also* Palmer, *supra* note 4, at 296 (emphasizing the vulnerabilities of critical infrastructure).

114. LEWIS, CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY, *supra* note 108, at 1.

115. *See, e.g.*, de Laat, *supra* note 112, at 452–53; *see also* Condron, *supra* note 4, at 406 (stating that the U.S. "government's approach to protect cyberspace focuses on the concept of 'critical infrastructure'").

116. *See, e.g.*, LEWIS, CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY, *supra* note 108, at 4.

117. Carter & Sofio, *supra* note 1, at 233, 238.

118. *See, e.g.*, Shackelford et al., *supra* note 2, at 32.

119. LEWIS, CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY, *supra* note 108, at 3.

120. The term "critical information infrastructure" in Cybersecurity Law is equivalent to "critical infrastructure" in most of the literature on the topic. *See* David Satola & Henry L. Judy, *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum*, 37 WM. MITCHELL L. REV. 1745, 1754 n.14 (2011).

121. Cybersecurity Law, *supra* note 8, art. 31.

destroyed, rendered dysfunctional, or leaked, might seriously endanger "national security, national welfare, the people's livelihood, or . . . public interest."[122] Although the law dictates that the State Council defines the specific scope and security protection measures of the critical information infrastructure,[123] concerns have been raised that these may be too broad[124] because the State Council has the discretion to decide whether a specific internet business has something to do with "national security, national welfare and the people's livelihood, or the public interest."[125] Therefore, one interpretation is that "[w]hat businesses fall under this rubric will likely be left to the government's discretion."[126] Companies that are key suppliers of critical information infrastructure or hold a significant amount of data related to Chinese citizens or entities may be defined as "critical information infrastructure operators" as well.[127] The scope of who and what can be considered a critical information infrastructure operator may even be broad enough to include food delivery companies.[128] Therefore, the broad language used in the law may also create the impression that it can be utilized for reasons only tangentially related to cybersecurity. Because of such heavy obligations imposed on critical information infrastructure by the new law, most companies are reluctant to be considered critical information infrastructure operators.[129] Moreover, the ambiguous language used in Article 31, especially the phrases "people's livelihood" and "public interest,"[130] has created significant

122. *Id.*

123. *Id.*

124. *See, e.g.*, Keally, *supra* note 89; Ramsey & Wootliff, *supra* note 11; *see also* Zhuang Pinghui, *China Pushes Through Cybersecurity Law Despite Foreign Business Fears*, SOUTH CHINA MORNING POST (Nov. 8, 2016, 10:29 AM), http://www.scmp.com/news/china/policies-politics/article/2043646/china-pushes-through-cybersecurity-legislation-heavily (citing the concern raised by Jacob Parker, vice president of the US-China Business Council, that the definition of "'critical information infrastructure operators' had expanded from previous drafts and could be widened further").

125. Cybersecurity Law, *supra* note 8, art. 31.

126. Li et al., *supra* note 11.

127. Ramsey & Wootliff, *supra* note 11.

128. Gidda, *supra* note 5; *see also* Chin & Dou, *supra* note 28 (reporting that "[t]he law drew criticism from foreign business groups due to the expansive list of sectors that are defined as part of China's 'critical information infrastructure'"); *China Adopts a Tough Cyber-Security Law*, *supra* note 27 ("[T]he law's definition of critical is absurdly expansive."); Parasol, *supra* note 60, at 90 (asserting that the term "'[c]ritical information infrastructure network operators' is a clear ambiguity" in the law).

129. *See* Chin & Dou, *supra* note 28.

130. Cybersecurity Law, *supra* note 8, art. 31 (defining "critical information infrastructure" as that which, if destroyed, rendered dysfunctional, or leaked, could seriously endanger "national security, national welfare, the people's livelihood, [or] . . . public interest").

uncertainties for companies given the hefty obligations for those considered critical information infrastructure operators.

Critical information infrastructure operators are a subset of network operators that bear more obligations than typical network operators. Pursuant to Article 34, these operators have the obligation to conduct security background checks on responsible personnel in critical positions, carry out cybersecurity education and technical training, and implement disaster recovery backups.[131] Critical information infrastructure operators are also required to conduct inspections of their network security on at least an annual basis.[132] Breaches of these duties may lead to critical information infrastructure operators being fined between RMB 100,000 and 1,000,000 (approximately $15,920 and $159,150, respectively), and the management personnel directly responsible may face fines between RMB 10,000 and 100,000 (approximately $1,590 and $15,920, respectively).[133]

There is no question that the private sector's cooperation and precautions are crucial to ensuring any country's cybersecurity.[134] However, how to best enable such measures in the private sector has been more difficult to determine in terms of cybersecurity policymaking. From a comparative perspective, because of congressional inaction, President Obama issued Executive Order 13,636 to facilitate public-private information sharing regarding the protection of critical infrastructure and to establish the National Institute of Standards and Technology ("NIST") Framework, which includes best practices for the private sector to secure critical infrastructure.[135] The NIST Framework consists of some overarching cybersecurity risk management principles that do not focus on a particular sector or entity.[136] Different from China's Cybersecurity Law, private critical infrastructure operators and owners do not have the legal duty to follow the NIST Framework.[137] Instead, these best practices are adopted on a voluntary basis.[138]

---

131. *Id.* art. 34.

132. *Id.* art. 38.

133. *Id.* art. 59 (currency conversions last updated Apr. 1, 2018).

134. *See* Gross, *supra* note 1, at 496–97.

135. NAT'L INST. OF STANDARDS & TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY: PRELIMINARY CYBERSECURITY FRAMEWORK 1 (2013), https://www.nist.gov/sites/default/files/documents/itl/preliminary-cybersecurity-framework.pdf [hereinafter NIST FRAMEWORK].

136. *See, e.g.*, Palmer, *supra* note 4, at 346.

137. *See, e.g.*, Carter & Sofio, *supra* note 1, at 234, 237; *see also* Etzioni, *supra* note 4, at 95–98 (documenting the difficulties associated with passing mandatory cybersecurity laws in the United States).

138. *See, e.g.*, Shackelford et al., *supra* note 2, at 35. *But see* John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, PIVOT POINT SECURITY (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework ("[I]f . . . cybersecurity practices [are] ever questioned

The contrast between China's mandatory and the United States' voluntary approaches illustrates the regulatory dilemma found in the protection of critical infrastructure. The Chinese Cybersecurity Law has created hefty obligations for private critical information infrastructure operators[139] that are too broadly defined.[140] This mandatory approach may create unnecessary compliance costs for a wide range of enterprises. However, the United States' voluntary approach is not without its flaws. Critics of the U.S. approach highlight that private enterprises are not sufficiently incentivized to take appropriate measures to protect critical infrastructure from cyberattacks[141] that will ultimately threaten national security.[142] As a result, some commentators doubt whether the voluntary scheme will be implemented effectively in order to protect cybersecurity associated with critical infrastructure.[143] Although the U.S. government once tried to develop a public-private partnership approach—charging the North American Electronic Reliability Corporation ("NERC") with developing and enforcing mandatory cybersecurity standards through collaboration with players in the electricity market—the model has not been successful.[144] Therefore, the most effective domestic regulatory approach to protecting critical infrastructure has yet to be developed.

---

during litigation or a regulatory investigation, the 'standard' for 'due diligence' [is] now the NIST Cybersecurity Framework.").

139. *See supra* text accompanying notes 131–33; *see also* Cybersecurity Law, *supra* note 8, art. 34 (requiring critical information infrastructure operators to conduct background checks of personnel in critical positions, routinely provide network security education and technical training for employees, implement disaster recovery backups, develop contingency plans for network security incidents and other risks, and comply with other obligations as prescribed by law); *id.* art. 36 (imposing confidentiality and security obligations on critical information infrastructure operators).

140. *See* Gidda, *supra* note 5; Ramsey & Wootliff, *supra* note 11; *supra* text accompanying notes 127–28; *see also* Chin & Dou, *supra* note 28 (reporting that "[t]he law drew criticism from foreign business groups due to the expansive list of sectors that are defined as part of China's 'critical information infrastructure'"); *China Adopts A Tough Cyber-Security Law*, *supra* note 27 ("[T]he law's definition of critical is absurdly expansive.").

141. *See, e.g.*, Palmer, *supra* note 4, at 347–48 (emphasizing that the voluntary scheme does not provide any liability protection or tax or other incentives that would encourage the industry to adopt those proposed principles).

142. *See, e.g.*, Carter & Sofio, *supra* note 1, at 236 (quoting Ralph Langner's criticism of the voluntary approach).

143. *Id.* at 237; *see also* Etzioni, *supra* note 4, at 95 (citing Christopher Cox, former chairman of the U.S. Security and Exchange Commission, as asserting that "[v]oluntary regulation [of cybersecurity] does not work"); Palmer, *supra* note 4, at 297 (introducing the debate on the advantages and disadvantages of mandatory and voluntary approaches to protecting critical infrastructure).

144. Palmer, *supra* note 4, at 339–40; *see also* SINGER & FRIEDMAN, *supra* note 7, at 201–02 (emphasizing that NERC does not have "an explicit responsibility to lead security initiatives").

C. Data Localization

"Data localization" typically refers to policies requiring companies to store data on users but only on servers within jurisdictional borders.[145] For example, certain countries—namely, Belgium, Denmark, Finland, Germany, Russia, Sweden, and the United Kingdom—all require financial data within a certain scope to be stored locally.[146] Some, including Australia and the United Kingdom, require health records to be stored within their borders.[147] Data localization is an important feature of China's Cybersecurity Law as it is based on the national government's claim to cyberspace sovereignty[148] and the assertion that requiring data to stay within the country's borders provides a higher level of security and protection.[149] Through data localization, governments can also more easily claim jurisdiction and exert control over data.[150] Although the protection of privacy and cybersecurity and the freedom from foreign surveillance are proclaimed as the policy goals of data localization,[151] it is also common for governments to implement such policies as a tool to support local data center industries or to facilitate domestic surveillance or law enforcement.[152] As a result, while data localization may not substantively increase the level of cybersecurity,

145. *See* Cohen et al., *supra* note 89, at 107; Sargsyan, *supra* note 34, at 2222; Selby, *supra* note 35, at 214; Reema Shah, Comment, *Law Enforcement and Data Privacy: A Forward-Looking Approach*, 125 YALE L.J. 543, 548 (2015); *see also* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 680 (2015) (defining "'data localization' measures as those that specifically encumber the transfer of data across national borders").

146. *See, e.g.*, Savelyev, *supra* note 80, at 129; Selby, *supra* note 35, at 226; *see also* Cohen et al., *supra* note 89, at 107.

147. *See, e.g.*, Chander & Lê, *supra* note 145, at 683, 719–20; Selby, *supra* note 35, at 226–27; *see also* Cohen et al., *supra* note 89, at 107.

148. *See, e.g.*, Selby, *supra* note 35, at 225; Tom Miles, *U.S. Asks China Not to Enforce Cyber Security Law*, REUTERS (Sept. 26, 2017, 7:22 AM), http://www.reuters.com/article/us-usa-china-cyber-trade/u-s-asks-china-not-to-enforce-cyber-security-law-idUSKCN1C11D1.

149. Cohen et al., *supra* note 89, at 107; Sacks, *supra* note 9.

150. Sargsyan, *supra* note 34, at 2224.

151. *See, e.g.*, Chander & Lê, *supra* note 145, at 679, 713; Sargsyan, *supra* note 34, at 2222, 2224–25, 2228; Savelyev, *supra* note 80, at 138; Shah, *supra* note 145; *see also* Lawrence Drewry, Note, *Crimes Without Culprits: Why the European Union Needs Data Retention, and How It Can Be Balanced with the Right to Privacy*, 33 WIS. INT'L L.J. 728, 752 (2016) ("The EU should . . . consider requiring utilities to store data within the EU . . . [to] ensure that the utilities are subject to compliance reviews, and thus that they are in fact complying with the data retention requirements. Additionally, this could protect the information from being exposed to jurisdictions with less accountability for the access of retained data.").

152. *See, e.g.*, Chander & Lê, *supra* note 145, at 713; Cohen et al., *supra* note 89, at 107–08; Sargsyan, *supra* note 34, at 2222–23; Selby, *supra* note 35, at 216, 225; Zhang, *supra* note 20.

it can effectively enable government surveillance and law enforcement in the online environment.[153]

According to Article 37, which is arguably "the most controversial provision" of the Cybersecurity Law,[154] critical information infrastructure operators are obliged to store personal information and other important data in China, and a security assessment or approval from relevant regulators is required before transferring this information or data abroad.[155] The penalty for failing to comply with this provision is at the very least a warning but may include website shutdown, license revocation, and fines ranging between RMB 50,000 and 5,000,000 (approximately $7,960 and $796,200, respectively) for businesses and RMB 10,000 and RMB 100,000 (approximately $1,590 and $15,920, respectively) for those in charge.[156] Commentators have viewed these rules as the strictest data localization requirements in the world.[157] In fact, China's data localization requirement has long been in place for some industries, such as the banking industry,[158] and, as a result, it has become a common practice in some industries.[159]

Most foreign companies have expressed consternation over the data localization requirement in China. Their first concern is that it creates considerable costs in terms of data management.[160] Multinational enterprises store their data on the cloud with servers in different jurisdictions to mitigate various efficiency, cost, or tax concerns.[161] Some companies even avoid physically locating their servers within the borders of repressive regimes, such as China, in

153. *See, e.g.*, Sargsyan, *supra* note 34, at 2223.

154. Gabriela Kennedy & Xiaoyan Zhang, *China Passes Cybersecurity Law*, 29 INTELL. PROP. & TECH. L.J. 20, 20 (2017); *see also* Charlie Campbell, *Baidu's Robin Li is Helping China Win the 21st Century*, TIME (Jan. 18, 2018), http://time.com/magazine/asia/5109057/january-29th-2018-vol-191-no-3-asia/ ("China rolled out a controversial new cybersecurity law that, among many stipulations, requires foreign companies doing business in the country to store related data locally."); Chin & Dou, *supra* note 28 (quoting Jared Ragland, senior director of policy for The Software Alliance, as expressing concern that the Cybersecurity Law's data localization requirements "could have a major impact on foreign companies"); O'Brien & Gruetzner, *supra* note 20 (stating that the data localization "provision is of most concern to the international business community" and is "[t]he new law's most onerous provision").

155. Cybersecurity Law, *supra* note 8, art. 37.

156. *Id.* art. 66 (currency conversions last updated Apr. 1, 2018).

157. Li et al., *supra* note 11; *see also* Selby, *supra* note 35, at 215, 221, 225 (describing China's data localization policy as one of the broadest in the world).

158. Chander & Lê, *supra* note 145, at 686; Zhang, *supra* note 20.

159. Sacks, *supra* note 9.

160. Josh Horwitz, *A Key Question is at the Heart of China's New Cybersecurity Law: Where Should Data Live?*, QUARTZ (June 7, 2017), https://qz.com/999613/a-key-question-at-the-heart-of-chinas-cybersecurity-law-where-should-data-live/.

161. *See, e.g.*, CHANDER, *supra* note 74, at 52–53; Savelyev, *supra* note 80, at 143; Shah, *supra* note 145, at 547.

order to avoid surveillance and censorship.[162] Because of the data localization policy, now such companies will need to build local data centers in China, seek local storage services,[163] or restructure or reconfigure their IT infrastructure.[164] For example, Apple has decided to outsource the storage of its Chinese iCloud users' data to the local firm Guizhou-Cloud Big Data, a state-owned enterprise affiliated with the Guizhou provincial government.[165] On the other hand, AsusTek, one of the largest personal computer manufacturers in the world, has made a completely opposite decision by withdrawing its Asus Cloud service from China because of compliance concerns arising from the Cybersecurity Law.[166] This new data localization requirement will definitely increase data storage costs for both internet businesses and consumers[167] because data centers are expensive to build.[168] With the data localization law, businesses classified as critical information infrastructure operators and their consumers will no longer be able to enjoy the efficiency provided by

162. *See, e.g.*, Sargsyan, *supra* note 34, at 2225.

163. *See* Gidda, *supra* note 5; *see also* Sargsyan, *supra* note 34, at 2222 ("Effectively, data localization proposals urge companies to alter their infrastructure by relocating or building new data centers in specific locations."); Selby, *supra* note 35, at 215 ("[D]ata localization . . . requires Internet content hosts to build or rent data centres in specified jurisdictions rather than to be able to choose wherever those data centres might be most logically located."); *China to Launch Cybersecurity Law Despite Concerns*, *supra* note 17 (reporting that China's Cybersecurity Law may impose "'new hurdles for foreign company compliance and operations' in industries, such as cloud computing, where China is actively seeking a competitive advantage").

164. *See, e.g.*, Savelyev, *supra* note 80, at 141; *see also* Zhang, *supra* note 20 (asserting that compliance with the Cybersecurity Law may bring about a "sweeping change in data architecture or infrastructure").

165. *See Apple: Chinese Firm to Operate China iCloud Accounts*, BBC NEWS (Jan. 10, 2018), http://www.bbc.com/news/business-42631386; Campbell, *supra* note 154; Josh Horwitz, *Apple's iCloud Service in China Will Be Managed by a Data Firm Started by the Government*, QUARTZ (Jan. 10, 2018), https://qz.com/1176376/apples-icloud-service-in-china-will-be-managed-by-a-data-firm-started-by-the-government/; Sherisse Pham, *Use iCloud in China? Prepare to Share Your Data with a State-Run Firm*, CNN (Jan. 11, 2018, 11:09 AM), http://money.cnn.com/2018/01/10/technology/apple-china-icloud/index.html; Don Reisinger, *Here's When Apple Will Hand Over Chinese iCloud Data to Comply With Local Laws*, FORTUNE (Jan. 10, 2018), http://fortune.com/2018/01/10/apple-china-icloud-data/.

166. Paul Huang, *In Sharp Contrast to Apple, Asus Bows Out of China's Cloud Storage Market to Protect Private User Data*, EPOCH TIMES (Feb. 15, 2018, 4:50 PM), https://m-news.theepochtimes.com/in-sharp-contrast-to-apple-asus-bows-out-of-chinas-cloud-storage-market-to-protect-private-user-data_2442490.html.

167. *See, e.g.*, Chander & Lê, *supra* note 145, at 681; Cohen et al., *supra* note 89, at 108; Savelyev, *supra* note 80, at 141–42; Shah, *supra* note 145, at 548–49; Chin & Dou, *supra* note 28; *China Adopts a Tough Cyber-Security Law*, *supra* note 27.

168. Chander & Lê, *supra* note 145, at 681.

the internet's distributed infrastructure or cloud technology.[169] From a macroeconomic perspective, the data localization provision in the Cybersecurity Law has been viewed as a trade barrier by some multinational enterprises,[170] and the legality of this provision under the international trade regime is already being challenged by the United States in the World Trade Organization.[171]

Domestic internet companies have raised similar concerns that data localization may prevent them from expanding globally. Jack Ma of Alibaba once complained that data localization regulations create a "major problem[] for Chinese internet companies expanding overseas . . . ultimately leading to the fragmentation of cyberspace."[172] This worry has been confirmed by recent internet law scholarship showing that the data localization policy may lead to the "Balkanization of the Internet" by fundamentally changing the internet architecture that has, until now, facilitated universal connectivity and the free flow of information.[173] Therefore, some commentators believe that the data localization provision in the Cybersecurity Law will hobble globalization efforts made by China's primary internet companies—namely, the "BAT" triopoly of Baidu, Alibaba, and Tencent.[174]

---

169. OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2017 SPECIAL 301 REPORT 34 (2017), https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF; Chander & Lê, *supra* note 145, at 728; Shah, *supra* note 145; *see also* Patrick S. Ryan et al., *When the Cloud Goes Local: The Global Problem with Data Localization*, 46 COMPUTER 54, 56 (2013); Savelyev, *supra* note 80, at 143; Zhang, *supra* note 20.

170. Merrion, *supra* note 19; *see also* Andrew D. Mitchell & Jarrod Hepburn, *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 YALE J.L. & TECH. 182, 196–207 (2017) (discussing whether restrictive data transfer measures breach the nondiscrimination and market access disciplines under the General Agreement on Trade in Services or if they can be justified under the general exception found in article XIV of the agreement).

171. Miles, *supra* note 148.

172. Sacks, *supra* note 9; *see also* Kennedy & Zhang, *supra* note 154 ("This [data localization requirement] in essence would mean a segregation of the global information system into one distinct system for China and one for the rest of the world."); O'Brien & Gruetzner, *supra* note 20 (warning that China's Cybersecurity Law "will further isolate the domestic internet from rest of the world" and its major impact on domestic internet companies "such as Tencent Holdings and Alibaba Group Holding [is that they] will find it harder to expand overseas").

173. Selby, *supra* note 35, at 215–17; Shah, *supra* note 145; *see also* Chander & Lê, *supra* note 145 ("[D]ata localization measures break up the World Wide Web, which was designed to share information across the globe . . . . Data localization would dramatically alter this fundamental architecture of the Internet."); Cohen et al., *supra* note 89, at 107 (stating that "the rise of [] data localization measures threatens to balkanize the global Internet [and] restrict both domestic and global trade").

174. O'Brien & Gruetzner, *supra* note 20.

Another concern raised as a result of the data localization requirement is the unmanageable risk of data leaks. Some multinational enterprises worry that the mandate will enable the Chinese government to access their proprietary information or trade secrets.[175] Also, companies are more vulnerable to government censorship and surveillance, which will ultimately threaten the privacy of their users.[176] Moreover, aggregating data in one location or jurisdiction may render it more susceptible to hacking attacks.[177] As a result, data localization may harm, rather than strengthen, cybersecurity.

A minor criticism of the data localization provision found in Article 37 is that, although the law defines "personal information,"[178] it does not define what constitutes "important data."[179] While the CAC defines "important data" as "data closely related to national security, economic development, and social public interest,"[180] it is quite possible that the government may define "national security, economic development, and social public interest" at its own discretion and consequently create enormous costs for business to comply with the data localization obligation. In addition, Article 37 contains no substantive definition of "security assessment"[181] and a relevant procedure for such an assessment has yet to be announced by the government.

In response to the concerns highlighted above, the Chinese government has indicated that data localization is not intended to hinder globalization under the One-Belt-One-Road initiative.[182] Zhao Zeliang of the CAC has made it clear that data localization will not block the transnational flow of data but will remind regulators and businesses of the risks associated with cross-border data transfers.[183] However, given the severe penalties attached to the data localization requirement in the Cybersecurity Law,[184] it is reasonable to expect

175. Sacks, *supra* note 9; *see also* Parasol, *supra* note 60, at 86 (indicating that "Article 37 has created fears of potential intellectual property theft in China").

176. *See, e.g.*, Sargsyan, *supra* note 34, at 2229.

177. *See, e.g.*, *id.*; *see also China Adopts a Tough Cyber-Security Law*, *supra* note 27 (noting that the Cybersecurity Law's data localization requirement will "increase the risk of data theft").

178. Cybersecurity Law, *supra* note 8, at art 76.5.

179. *See, e.g.*, Cohen et al., *supra* note 89, at 110; Zhang, *supra* note 20; Sophia Yan, *China's New Cybersecurity Law Takes Effect Today, and Many Are Confused*, CNBC (June 1, 2017, 3:15 AM), https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html.

180. (个人信息和重要数据出境安全评估办法 (征求意见稿)) [Guidelines for Security Assessment of Cross-Border Transfer of Personal Information and Important Data (Consultation Draft)], (promulgated by the Cyberspace Admin. of China, Apr. 11, 2017), art. 17.

181. *See, e.g.*, Nick Akerman et al., *Fall 2016 Cross-Border Data Privacy Issues*, 25 CARDOZO J. INT'L & COMP. L. 379, 414 (2017); Zhang, *supra* note 20.

182. Sacks, *supra* note 9.

183. *Id.*

184. *See supra* text accompanying note 156.

that the transnational flow of data from China will be significantly reduced. It will be worth observing how the Chinese government will trade off its policy goal of data localization while maintaining its global technological ambitions.

D. Security Certification, Inspection, and Review

Cybersecurity can be ensured only when critical information infrastructure operators and other network operators adopt products and services that meet certain security standards. Therefore, determining which standards should be adopted has been a crucial issue in cybersecurity policy. China developed a set of cybersecurity standards in 2007 in the Regulations on Classified Protection of Information Security, which are referred to as the Multiple-Level Protection Scheme ("MLPS").[185] Nevertheless, the MLPS was criticized as being inconsistent with international cybersecurity standards and described as little more than protectionist measures to guard domestic companies from global competition.[186]

The Cybersecurity Law includes a complicated security certification, inspection, and review regime. Article 23 stipulates that critical network equipment and specialized network security products shall follow the national standards and mandatory requirements, with the security level certified by a qualified institute or confirmed by security inspection.[187] The provision further requires that the state's network information departments, together with the relevant departments of the State Council, to formulate and release a catalog of critical network equipment and specialized network security products as well as promote the reciprocal recognition of security certifications and security inspection results to avoid duplicative certifications and inspections.[188]

Under Article 35, network products and services purchased by critical information infrastructure operators that might affect national security are required to undergo a national security review by the government.[189] The obligations imposed by Articles 23 and 35 are evidently onerous and time-consuming. In order to implement Article 35, the CAC released the Measures on the Security Review of Network Products and Services (Interim)—also referred to as the "Interim Measures"—on May 2, 2017.[190] According to the Interim Measures, the CAC will establish a committee to conduct the security reviews,[191] and the focus of such reviews will be on whether the

185. Shackelford et al., *supra* note 2, at 32.
186. *Id.* at 32–33.
187. Cybersecurity Law, *supra* note 8, art. 23.
188. *Id.*
189. *Id.* art. 35.
190. (网络产品和服务安全审查办法（试行)) [Measures on the Security Review of Network Products and Services (Interim)], (promulgated by the Cyberspace Admin. of China, May 2, 2017) [hereinafter Interim Measures].
191. *Id.* art. 5.

products and services are secure and controllable.[192] The Interim Measures list several approaches to security review, including laboratory testing, onsite inspection, online monitoring, and background investigation.[193] Nevertheless, the true meaning of these approaches remains unclear. Although source code disclosure was previously removed from drafts of the Chinese regulations,[194] it is still not clear whether the relevant committee can legally ask product or service vendors to provide source code or install backdoors in hardware and software,[195] which has been mandated in the Chinese banking industry since December 2014.[196] Moreover, the Interim Measures neither identify what type of information will be collected from the security review nor specify any appeals or remediation processes that can be followed if the products or services do not pass the security review.[197] According to the Interim Measures, the scope of the security review also includes "risks that could harm national

192. *Id.* art. 4. It should be noted that the Chinese government required the country's banking industry to employ secure and controllable IT products before the enactment of Cybersecurity Law. *See, e.g.*, Nan-xiang Sun, *Piercing the Veil of National Security: Does China's Banking IT Security Regulation Violate the TBT Agreement?*, 11 ASIAN J. WTO & INT'L HEALTH L. & POL'Y 395, 401–02 (2016). Moreover, according to the Outline of the National Informatization Development Strategy released by the Chinese government in July 2016, China must build secure and controllable information technology systems in order to lead globally in next-generation mobile telecommunications and next-generation internet and other such areas and must strive to build comparative advantages in areas such as mobile internet, cloud computing, big data, etc. (国家信息化发展战略纲要) [Outline of the National Informatization Development Strategy] (promulgated by the State Council General Office, July 27, 2016), http://www.gov.cn/xinwen/2016-07/27/content_5095336.htm.

193. Interim Measures, *supra* note 190, art. 3.

194. Chin & Dou, *supra* note 28.

195. Pinghui, *supra* note 124; *see also* Blake, *supra* note 21 (noting that "Microsoft, Intel, and IBM are formally opposing a new cybersecurity law that could potentially force tech companies to supply the Chinese government with their product's proprietary source code"); Chin & Dou, *supra* note 28 ("The security reviews stipulated in the new law revive concerns among U.S. companies that they will be forced to disclose their source code."); *China Adopts a Tough Cyber-Security Law*, *supra* note 27 (reporting that foreign firms fear that security certifications provisions may "be used to force them to turn over security keys"); Nicole Lindsey, *China's Cybersecurity Law Pushes Cyber Sovereignty Vision*, CPO MAGAZINE (Jan. 8, 2018), https://www.cpomagazine.com/2018/01/08/chinas-cybersecurity-law-pushes-cyber-sovereignty-vision/ (indicating that "the intellectual property risk of China's Cybersecurity Law is that random security assessment spot-checks required by the Chinese authorities could be used to force foreign companies to hand over source code, encryption information or sensitive network security data to the Chinese government"); Zhang, *supra* note 20 (stating that the "safe and trustworthy" standard is "generally understood to mandate source code reviews, turn-over of encryption keys, and/or access to 'backdoors' for government inspections").

196. Yuen, *supra* note 61, at 56–57; *see, e.g.*, Shackelford et al., *supra* note 2, at 33 (describing similar legislation that has been recently proposed in China).

197. Interim Measures, *supra* note 190, art. 3.

security."[198] This broad statement could be a catch-all provision that the government may use for its political purposes.

The purpose of these regulations is to reduce cybersecurity threats or, more specifically, to prevent products and services from being manipulated by foreign forces.[199] China believes that its digital network will be more vulnerable to cyberattacks if its components are manufactured by foreign firms.[200] Nonetheless, the Interim Measures have been criticized as being unclear in their "substantive criteria and procedure" as related to the security review process.[201] Undoubtedly, a comprehensive security inspection regime may enable ubiquitous digital surveillance.[202] Companies have expressed concern that mandated security inspection, certification, and review may create more opportunities for the leakage of trade secrets and other confidential information regarding information security.[203] The Office of the United States Trade Representative raised similar concerns in its 2017 Special 301 Report, specifically that companies may be obliged to disclose proprietary intellectual property to comply with the security review requirement.[204] Furthermore, the security certification, inspection, and review requirements in Articles 23 and 35 may inappropriately intervene in the market, as each of these requirements may be used for political purposes to delay or block market access to industries that are defined as critical information

198. *Id.* art. 4.5.

199. Richard Hoffmann, *Update: China Releases New Draft Regulations Regarding Cyber Security of Online Services and Products*, ECOVIS BEIJING (Feb. 8, 2017), http://www.ecovis-beijing.com/en/blog-en/articles/810-update-china-releases-new-draft-regulations-regarding-cyber-security-of-online-services-and-products; *see also* Yuen, *supra* note 61, at 56 (indicating that, with regard to cybersecurity, the Chinese government "has become increasingly cautious against foreign technology").

200. Yuen, *supra* note 61, at 57.

201. Yan Luo, *China Releases Final Regulation on Cybersecurity Review of Network Products and Services*, COVINGTON: INSIDE PRIVACY (May 2, 2017), https://www.insideprivacy.com/international/china/china-releases-final-regulation-on-cybersecurity-review-of-network-products-and-services/.

202. *Cf.* Yuen, *supra* note 61, at 57 (noting that Human Rights Watch criticized the Chinese cybersecurity regulations as "enforcing a system of complete, permanent digital surveillance").

203. *See, e.g.*, Chin & Dou, *supra* note 28 (describing foreign companies' concerns over trade secret leakage caused by security reviews); *China Adopts a Tough Cyber-Security Law*, *supra* note 27 (noting foreign companies' fear that the law's security certification provisions may "be used to force them to turn over . . . proprietary technologies, which could be passed on to state-owned rivals"); *China to Launch Cybersecurity Law Despite Concerns*, *supra* note 17 (raising the concern that "companies with politically well-connected competitors could see their profile raised for things such as cybersecurity reviews"); Pinghui, *supra* note 124 (asserting that the Cybersecurity Law's security review clauses have "raise[d] concerns within foreign companies that they would have to hand over intellectual property . . . to operate in China").

204. OFFICE OF THE U.S. TRADE REPRESENTATIVE, *supra* note 169, at 34–35.

infrastructure.[205] Concerns have also been raised that these requirements may affect enterprises' decisions when purchasing security products and services.[206] These regulations may have been designed to form an industrial policy to reduce the country's reliance on foreign cybersecurity technology[207] and spur investment in the domestic information industry, which has grown significantly over the past two decades.[208]

E. Personal Data Regime

Striking a balance between cybersecurity, national security, and privacy protection has posed a considerable challenge for all nation-states.[209] Before the enactment of the Cybersecurity Law, the Chinese government issued a series of rules for personal data protection, including the Decision of the Standing Committee of the National People's Congress to Strengthen the Protection of Internet Data (2012),[210] the Guidelines for Personal Information Protection within Public and Commercial Services Information Systems

205. *Cf. China to Launch Cybersecurity Law Despite Concerns*, *supra* note 17 ("Companies are worried that the new [Cybersecurity Law] could lock them out of market."); Mozur, *supra* note 82 (warning that the law's security inspection provisions will "lock [companies] out altogether"). *But see* OFFICE OF THE U.S. TRADE REPRESENTATIVE, *supra* note 169, at 34 ("China explained that its secure and controllable policies generally applicable to the commercial sector are not to unnecessarily limit or prevent commercial sales opportunities for foreign suppliers, of [information and communications technology ("ICT")] products, services, or technologies and will not impose nationality-based conditions and restrictions on the purchase, sale, and use of ICT by commercial enterprises unnecessarily.").

206. *See, e.g.*, *China's Tough Cybersecurity Law to Come into Force This Week*, SOUTH CHINA MORNING POST (May 29, 2017, 3:41 PM), http://www.scmp.com/news/china/policies-politics/article/2096094/chinas-tough-cybersecurity-law-come-force-week (reporting that such concerns are already "tilting purchasing decisions").

207. *See, e.g.*, Haour, *supra* note 27 (claiming that the Cybersecurity Law promotes "indigenous innovation" and favors Chinese firms "by establishing non-tariff barriers—such as specific standards or regulations on products"); *cf.* Yuen, *supra* note 61, at 57 ("[G]rowing caution against foreign technology is shaping a new wave of technological development in China . . . . [C]ybersecurity concerns have become an impetus for the Chinese government to reduce reliance on foreign [technology] . . . and encourage development of domestic [technology].").

208. *See* Lindsay, *supra* note 32, at 18.

209. *See, e.g.*, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 165–67 (2012); SINGER & FRIEDMAN, *supra* note 7, at 3, 106–07; Harrop & Matteson, *supra* note 4, at 164; Palmer, *supra* note 4, at 356–58; Tene, *supra* note 1, at 392, 417; *see also* Hurwitz, *supra* note 101, at 423 ("It is difficult to find the correct balance between the right of individuals to be secure against government intrusion and the need of the government to sometimes encroach upon that right.").

210. Nir Kshetri, *Cybercrime and Cybersecurity Issues in the BRICS Economies*, 18 J. GLOBAL INFO. TECH. MGMT. 245, 247 (2015).

(2013),[211] and the Provisions on Protecting the Personal Information of Telecommunication and Internet Users (2013).[212] The Cybersecurity Law provides citizens with an unprecedented amount of protection to ensure their data privacy.[213] The law defines "personal information" as information that can be used on its own or in conjunction with other information to determine the identity of a natural person, including but not limited to a person's name, birthday, identity card number, biological identification information, address, and telephone number.[214] In other words, once such information is deidentified, it will no longer be subject to the requirement for personal information in the Cybersecurity Law.

According to the Cybersecurity Law, network operators' collection and use of personal information must be legal, proper, and necessary.[215] Network operators are also required to disclose the purpose, methods, and scope of their data collection and obtain the consent of the persons whose information is collected.[216] Data subjects are afforded the right under the law to access, modify, and delete their personal information.[217] Personal information that is irrelevant to the service provided may not be collected.[218] Network operators are prohibited from disclosing personal information collected pursuant to the law to any other party unless (1) the person whose information was collected gives their consent or (2) the information has been processed in a manner so that the particular individual is unidentifiable and no recognizable information can be recovered.[219] Moreover, network operators shall not disclose, alter, or destroy the personal information they collect under the Cybersecurity

211. *Id.*; James D. Fry, *Privacy, Predictability and Internet Surveillance in the U.S. and China: Better the Devil You Know?*, U. PA. J. INT'L L. 419, 480 (2016); Sargsyan, *supra* note 34, at 2226.

212. Fry, *supra* note 211, at 494–95.

213. *See, e.g.*, Iasiello, *supra* note 20, at 7 (noting that "most of the privacy enhancements benefiting Chinese citizens . . . align with those required in the European Union"); Kennedy & Zhang, *supra* note 154, at 20–21 ("As China's first comprehensive privacy . . . regulation for cyberspace, the [Cybersecurity Law] enhances data protection in many aspects [and] makes progress by addressing many specific privacy aspects."); *see also* Yan, *supra* note 179 (reporting that "[t]he law has been largely touted by Beijing as a milestone in data privacy regulations").

214. Cybersecurity Law, *supra* note 8, art. 76.5.

215. *Id.* art. 41.

216. *Id.*

217. *Id.* art. 43 ("Individuals [who] discover[] that network operators, in violation of . . . laws and administrative regulations or both parties' agreement, collect and use their personal information are entitled to require network operators to delete their personal information . . . . Network operators should take measures to [delete or correct such information accordingly].").

218. *Id.* art. 41.2.

219. *Id.* art. 42.1.

Law.[220] In the event of a data breach or potential data breach, network operators must take remedial action, promptly inform users, and report to the competent authorities.[221]

Although the law has enhanced privacy protection by imposing legal obligations on network operators, it does not seem to oblige public authorities to uphold the same standards.[222] Instead, other provisions in the Cybersecurity Law that provide the government with legal instruments to control and surveil personal information held by various network operators have imposed significant risks on privacy protection. For example, as mentioned previously, network operators are obliged to provide technical support and assistance to public security authorities and state security authorities for the purposes of lawfully upholding national security and investigating crimes.[223] This obligation has exposed personal data held by network operators to a high risk of leakage.[224] If governments can legally mandate that network products and service providers build backdoors into hardware and software, or provide access to these backdoors,[225] the risk of privacy infringement will increase even more significantly. Similarly, network operators' obligation to store network logs for at least six months[226] also threatens the protection of personal information. While data retention regulations are increasingly common,[227] and most international internet companies retain identifying user log data for the purposes of law enforcement,[228] the six-month retention period in the Cybersecurity Law will certainly generate considerable costs for network operators—especially small companies.[229] Moreover, all log retention policies or regulations will impact users' privacy because their personal information will be exposed to a higher risk of leakage.[230]

---

220. *Id.* art. 42.2 ("Network operators should take technical measures and other necessary measures to ensure that the personal information collected by them is safe and prevent the information from being leaked, damaged, or lost.").

221. *Id.*

222. PERRY & RODA, *supra* note 61, at 107.

223. Cybersecurity Law, *supra* note 8, art. 28; *see supra* text accompanying note 100.

224. *See supra* text accompanying notes 101–03.

225. *See supra* text accompanying note 196.

226. Cybersecurity Law, *supra* note 8, art. 21; *see supra* text accompanying note 91.

227. *See* Gus Hosein, *Returning to a Principled Basis for Data Protection*, 84 CHI.-KENT L. REV. 803, 803–04 (2010).

228. *See* Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, 12 MINN. J.L. SCI. & TECH. 191, 212 (2011).

229. *See* Ruan, *supra* note 27.

230. *See* Soghoian, *supra* note 228, at 196; *see also* Hosein, *supra* note 227, at 804 (summarizing privacy advocates' perspective that "data retention invades the privacy of Europeans, that it is illegal under the European Convention on Human Rights, threatens consumer confidence, burdens European industry, and will require even more invasive laws to make it work").

The new law includes preexisting local and national real-name registration policies,[231] which demand that network operators require users to disclose their real names and personal information.[232] Specifically, the Cybersecurity Law bars network operators from providing services to users who refuse to reveal their true identities.[233] The official justification for the real-name registration obligation is that, by helping to eliminate rumors, vulgarity, pornography, and information related to terrorism, information security and a safer and healthier internet can be ensured.[234] Nonetheless, China's real-name registration regime has been viewed as a government tool to prevent internet users from criticizing government officials or publicizing government corruption.[235] As such, this system may create a chilling effect by which outspoken individuals will be discouraged to comment on public affairs.[236] In addition, the implementation of real-name registration rules may pose a serious risk to privacy protection[237] by creating opportunities for hackers to steal identity information from various network operators.[238]

IV. EVALUATION OF THE CYBERSECURITY LAW

The Cybersecurity Law presents China's regulatory approach to cybersecurity and digital human rights and reflects the nation-state's distrust in the market's approach cybersecurity and national security. The vague language the law employs has created great uncertainty for the industry and given interpretive flexibility to regulators. This Part provides an overall policy analysis and evaluation of the Cybersecurity Law to illustrate China's unique perception of cybersecurity.

A. The Chinese Version of Cybersecurity

The Cybersecurity Law covers a broad range of industries that occasionally fall outside of the internet and information security industries.[239] The data and information subject to regulatory control are also wide-ranging.[240] Moreover, concerns have been raised that the government may use the law and the notion of cybersecurity to

231. Cybersecurity Law, *supra* note 8, art. 24; *see also* Lee & Liu, *supra* note 2, at 11–15.
232. Cybersecurity Law, *supra* note 8, art. 24.
233. *Id.*
234. *See* Lee & Liu, *supra* note 2, at 15–16; *see also* Yuen, *supra* note 61, at 55.
235. Lee & Liu, *supra* note 2, at 16.
236. *See, e.g.*, Yuen, *supra* note 61, at 55.
237. Lee & Liu, *supra* note 2, at 18–19.
238. *Id.*
239. *See, e.g.*, *supra* text accompanying notes 87–90, 120–28.
240. *See, e.g.*, *supra* text accompanying notes 178–81.

conduct surveillance,[241] acquire confidential information held by the private sector,[242] or block market access.[243] Therefore, the law seems to have extended beyond the aim of ensuring cybersecurity.

One may argue that the Chinese government actually intends to use the new law to fulfill its political agenda rather than protect its cybersecurity. However, the far-reaching scope of the Cybersecurity Law can also be explained by recognizing how China's conception of cybersecurity differs from that of the Western world. The Western idea of cybersecurity places a greater emphasis on technical threats, whereas the Chinese notion of cybersecurity prioritizes ideological threats.[244] In addition to the security of networks and information systems, China's cybersecurity policy also covers censorship and "properly guiding Internet opinion."[245] The inclusive view of cybersecurity is essential to understanding China's approach to relevant legislation and policy. The country's unique regulatory mindset explains why President Xi Jinping has associated cybersecurity with a healthy internet culture.[246] In a white paper published by China's State Council Information Office in 2010, the government asserted that among its policy goals in protecting cybersecurity—or internet information security—is to eliminate all online content that can be described as

> being against the cardinal principles set forth in the Constitution; endangering state security, divulging state secrets, subverting state power and jeopardizing national unification; damaging state honor and interests; instigating ethnic hatred or discrimination and jeopardizing ethnic unity;

241. *See supra* text accompanying note 30; Parasol, *supra* note 60, at 89–91; *see also* Iasiello, *supra* note 20, at 1 (stating that many critics believe that "China is seeking to increase its control over domestic Internet activity and the information traversing it" via the Cybersecurity Law); *cf.* Lewis, *supra* note 46, at 490 (noting that "the PRC government will use security as justification for censoring peaceful government criticism posted on the Internet"); Shackelford et al., *supra* note 2, at 30 (suggesting that China has attempted to shape the international norm with regard to censorship "under the guise of information security").

242. *See, e.g.*, *supra* text accompanying notes 101–03.

243. *See, e.g.*, *supra* text accompanying notes 205–06; *see also* Parasol, *supra* note 60, at 77 (contemplating whether the law "restrict[s] market entry by . . . making compliance too onerous").

244. Lindsay, *supra* note 32, at 15; *see also* Iasiello, *supra* note 20, at 2 ("While the United States maintains a technological view of cyberspace, China is more holistic in its perception taking into account not only the technology that facilitates communications, but also the actual data traverses or is stored on it."); Chen, *supra* note 39 (citing Zhang Lifan, a historian and frequent political commentator, as concluding that the government has linked cybersecurity with ideological issues).

245. Shackelford et al., *supra* note 2, at 31.

246. *Filthy, Polluted Cybersphere Not in Anyone's Interests, Xi Says*, XINHUA NEWS (Apr. 19, 2016), http://news.xinhuanet.com/english/2016-04/19/c_135294056.htm.

> jeopardizing state religious policy, propagating heretical or superstitious ideas; spreading rumors, disrupting social order and stability; disseminating obscenity, pornography, gambling, violence, brutality and terror or abetting crime; humiliating or slandering others, trespassing on the lawful rights and interests of others; and other contents forbidden by laws and administrative regulations.[247]

This statement clearly reflects China's perspective on cybersecurity, which concerns the maintenance of social stability, state power, and national unification.[248]

The unique Chinese approach to cybersecurity can also be found in the International Code of Conduct for Information Security proposed by China, Russia, Tajikistan, and Uzbekistan at the United Nations General Assembly in September 2011.[249] In order to maintain global information security, the code asked countries to collaborate to combat "criminal and terrorist activities," which included "curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."[250] Although the proposed code was rejected by the United States,[251] the wording used in the code clearly reflected China's perception of cybersecurity as encompassing content control and supporting an ideology that maintains social stability.[252]

A similar clue from the Cybersecurity Law includes the network operators' real-name registration obligation, through which the government has connected cybersecurity to a healthy internet environment in which rumors, vulgarity, and other unhealthy information should be eliminated.[253] The Cybersecurity Law also

---

247. INFO. OFFICE OF THE STATE COUNCIL OF CHINA, *supra* note 67, at pt. V.

248. *Id.*

249. U.N. GAOR, 66th Sess., at 1, U.N. Doc. A/66/359 (Sept. 14, 2011) [hereinafter U.N. Doc. A/66/359].

250. *Id.* at 4.

251. Statement of the Delegation of the United States of America to the Other Disarmament Issues and International Security Segment of Thematic Debate in the First Committee of the Sixty-Seventh Session of the United Nations General Assembly (Nov. 2, 2012), https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/assets/special/meetings/firstcommittee/67/pdfs/Thematic/01%20Nov%20TD%20Clust%205%20USA.pdf.

252. *See* U.N. Doc. A/66/359, *supra* note 249, at 4 (stating that "information and communications technologies" should not be used "to carry out hostile activities" and that international cooperation is needed to uphold "social stability").

253. *See supra* text accompanying note 234; *see also* Kshetri, *supra* note 210, at 246 ("China and Russia view information security as much broader than [a] cybersecurity issue. A real purpose is arguably to increase the state's capacity and legitimacy for cyber-control and censorship.").

comprises a child-safety protection clause[254] that has rarely been seen in cybersecurity legislation in other countries. Moreover, the prohibited behaviors that threaten cybersecurity in the law include

> us[ing] the network to engage in activities endangering national security, honor, and interests; inciting subversion of national sovereignty and the overturn of the socialist system; inciting separatism or undermining national unity; advocating terrorism or extremism; inciting ethnic hatred and ethnic discrimination; disseminating violent, obscene, or sexual information; creating or disseminating false information to disrupt the economic or social order; infringing on the reputation, privacy, intellectual property, or other lawful rights and interests of others; and other such acts.[255]

Since the law came into effect, much attention has been focused on its provisions governing content control and newly released regulations, such as the Internet News Service Management Regulations and the Regulations for Internet Content Management Administration Law Enforcement Procedures.[256] The government's attempt to purify online content through the Cybersecurity Law is evidenced by the CAC's recent imposition of huge fines on the country's three major internet companies—Tencent, Baidu, and Sina.[257] The three internet giants were held in violation of the Cybersecurity Law because they failed to properly manage their social media platforms as some users "spread information of violence and terror, false rumors, pornography, and other information that jeopardizes national security, public safety, and social order."[258] Similarly, Marriott International, the hotel operator, was found in violation of the Cybersecurity Law and advertising regulations, in response to which the Shanghai Internet Information Office shut down the company's Chinese website and mobile apps for a week.[259] What Marriot did was

254. *See, e.g.*, Cybersecurity Law, *supra* note 8, art. 13 ("The state encourages research and development of network products and services conducive to the healthy upbringing of minors [and will] lawfully punish[] [those who] exploit networks to engage in activities that endanger the psychological and physical wellbeing of minors.").

255. *Id.* art. 12.

256. Samm Sacks & Paul Triolo, *Shrinking Anonymity in Chinese Cyberspace*, LAWFARE (Sept. 25, 2017, 12:29 PM), https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace.

257. Charlotte Gao, *China Fines Its Top 3 Internet Giants for Violating Cybersecurity Law*, DIPLOMAT (Sept. 26, 2017), https://thediplomat.com/2017/09/china-fines-its-top-3-internet-giants-for-violating-cybersecurity-law/.

258. *Id.*

259. *See* Pei Li & Brenda Goh, *Shanghai Temporarily Closes Marriott Website in China After Questionnaire Gaffe*, REUTERS (Jan. 11, 2018, 3:47 AM), https://www.reuters.com/article/us-china-marriott/shanghai-temporarily-closes-marriott-website-in-china-after-questionnaire-gaffe-idUSKBN1F00UT; Wayne Ma, *Marriott Makes China Mad with Geopolitical Faux Pas*, WALL ST. J. (Jan. 12, 2018, 10:26 PM), https://www.wsj.com/articles/location-location-chinese-officials

not directly associated with cybersecurity in the traditional sense but involved listing Hong Kong, Macau, Taiwan, and Tibet as separate countries in a survey distributed to customers.[260] This conduct was viewed by the government as an indication of support for secession movements and a threat to Chinese sovereignty and territorial integrity.[261] In sum, the excessively broad range of behaviors regulated by the Cybersecurity Law definitely extends far beyond the scope of what is normally perceived as constituting cybersecurity in other countries.

For the Chinese authorities, protecting cybersecurity also helps to maintain social and political stability,[262] which may help strengthen the Communist Party of China's ongoing control of the state.[263] Therefore, any online behavior or information that may endanger social or political stability will be viewed as a threat to cybersecurity, and the concept of cybersecurity in China consequently is much broader than that in the Western world.[264] With its ties to ideology and social stability,[265] the Cybersecurity Law should be

---

-slam-marriotts-designation-of-hong-kong-macau-as-countries-1515663854; Alanna Petroff & Steven Jiang, *China Blocks Marriott for Listing Tibet and Taiwan as Countries*, CNN MONEY (Jan. 11, 2018, 12:56 PM), http://money.cnn.com/2018/01/11/news/companies/marriott-china-website-app-blocked-tibet-taiwan/index.html; Sui-Lee Wee, *Marriott to China: We Do Not Support Separatists*, N.Y. TIMES (Jan. 11, 2018), https://www.nytimes.com/2018/01/11/business/china-marriott-tibet-taiwan.html; Xu Junqian, *Marriott Website Shut for Cleanup*, CHINA DAILY (Jan. 12, 2018, 8:47 AM), http://usa.chinadaily.com.cn/a/201801/12/WS5a5805a0a3102c394518eade.html.

260. *Chinese Probe into Marriott Hotels over Geography Gaffe in Customer Survey*, SOUTH CHINA MORNING POST (Jan. 11, 2018, 11:50 PM), http://www.scmp.com/news/china/policies-politics/article/2127800/chinese-probe-marriott-hotels-over-geography-gaffe; Li & Goh, *supra* note 259; Ma, *supra* note 259; Petroff & Jiang, *supra* note 259; Wee, *supra* note 259; Xu, *supra* note 259.

261. *See, e.g.*, Li & Goh, *supra* note 259; Ma, *supra* note 259; Petroff & Jiang, *supra* note 259; Wee, *supra* note 259.

262. Shackelford et al., *supra* note 2, at 31–32; Chen, *supra* note 39; *see also* SINGER & FRIEDMAN, *supra* note 7, at 107 (indicating that the Chinese government has viewed censorship as a tool for stability rather than a violation of human rights); Yu Hong, *Reading the 13th Five-Year Plan: Reflections on China's ICT Policy*, 11 INT'L J. COMM. 1755, 1767 (2017) (describing the link between cybersecurity and social stability in China's 13th Five-Year Plan); Orji, *supra* note 74 (indicating that "China considers the preservation of its social-political . . . traditions . . . as a part of its cybersecurity initiatives").

263. *See, e.g.*, Iasiello, *supra* note 20, at 3 (noting that China's cybersecurity strategy is ultimately intended to "preserv[e] the Chinese Communist Party in power"); Ruan, *supra* note 27 (citing a Chinese historian's opinion that the Cybersecurity Law represents the authoritarian state's "effort to secure the regime and its power"); *see also* Jiang, *supra* note 59, at 72–73 (suggesting that Beijing's internet policy is rooted in its "fundamental interest in maintaining regime legitimacy by delivering economic growth and domestic stability" and that it poses "minimal political risk for the one-party state").

264. Shackelford et al., *supra* note 2, at 31.

265. *See, e.g.*, Leyden, *supra* note 79 (citing Bill Hagestad, an expert in cybersecurity, as asserting that the Cybersecurity Law is "designed to ensure the

interpreted alongside China's other internet regulations and the Great Firewall.[266] All the regulations and architecture aiming to restrict the flow of information are designed primarily to support authoritarian control.

B. Market Intervention

The Chinese government's regulation of market activities has also been a focus of internet law scholarship.[267] China's Great Firewall has notably intervened in the online market by blocking foreign internet services provided by Google, Facebook, YouTube, and other multinational internet companies.[268] The Chinese government has further expressed its strong will to intervene in the market through many of the Cybersecurity Law's provisions. For example, the data localization requirement prevents critical information infrastructure operators from using more efficient cloud services that store data abroad.[269] Some researchers argue that the data localization rule actually decreases cybersecurity because when companies' storage options are limited to choosing local storage services or building their own, they lose the opportunity to deploy the most secure storage services that have survived global competition.[270]

The same argument can be applied to cybersecurity standards primarily developed or decided by the government. As leading cybersecurity companies, such as Kaspersky and Symantec, are not allowed to sell their products to financial institutions and critical information infrastructure operators, China has become more vulnerable to cyberattacks.[271] Some other commentators suggest that the government should not intervene in the market on cybersecurity issues because the private sector has more agility and knowledge to enhance cybersecurity.[272] The same argument can also be used to criticize the security certification, inspection, and review provisions in the Cybersecurity Law, which stipulate that the government has the power to decide which cybersecurity products and services are

---

Communist Party ideals are not directly or indirectly challenged by impure thoughts").

266. *See* Lee & Liu, *supra* note 74, at 148–49 (discussing regulations involving intermediaries before the Cybersecurity Law was enacted); *see also* Shackelford et al., *supra* note 2, at 14 (discussing the Great Firewall).

267. LAWRENCE LESSIG, CODE VERSION 2.0, at 124–28 (2006); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 513–14 (1999).

268. *See, e.g.*, Yuen, *supra* note 61, at 57–58.

269. *See supra* text accompanying notes 154–64. *But see* CHANDER, *supra* note 74, at 54 (asserting that "[c]loud computing seems to defy law").

270. Chander & Lê, *supra* note 145, at 716–17.

271. Shackelford et al., *supra* note 2, at 32–33; *see also China Adopts A Tough Cyber-Security Law*, *supra* note 27 (quoting Eric Xu, co-chief executive of Huawei, as asserting that "[i]f we're not open, if we don't bring in the world's best technology, we'll never have true information security").

272. *See, e.g.*, Tene, *supra* note 1, at 419.

adopted by critical information infrastructure operators.[273] The Cybersecurity Law and similar regulations represent distrust in the market, in which critical information infrastructure operators are supposed to be able to find the best cybersecurity products and services to meet their needs.

Although the market can usually provide an ideal solution, sometimes the law still needs to intervene. The point here is to question why the law needs to respond in some situations.[274] The justification for government intervention in the Cybersecurity Law may be that although critical information infrastructure operators need to satisfy the market demand for cybersecurity, their expectations of the level of cybersecurity is occasionally lower than that of the government. In other words, while businesses should be keen to protect their networks and confidential information from cyberattacks, they evaluate the factors that affect the level of cybersecurity differently than governments do. After all, cybersecurity in the business context is not always equal to that at the national security level.[275] Investment in cybersecurity may occasionally become costly and lead to nonproductive assets, which in turn will not yield any profit.[276] Consequently, businesses sometimes fail to seek higher levels of cybersecurity because of cost, profit, or other commercial concerns.[277] Such compromises could create considerable risks in terms of national security. Moreover, although cloud computing can save businesses from paying enormous data storage costs, from a technical perspective, cloud storage is vulnerable to a variety of cybersecurity threats associated with hacking.[278] Lastly, as mentioned previously, the government may use security certification, inspection, and review to block foreign companies' access

273. Cybersecurity Law, *supra* note 8, at arts. 23, 35.

274. *See* Lessig, *supra* note 267, at 522–23.

275. *See, e.g.*, Etzioni, *supra* note 4, at 95; *see also* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 513–14 (2017) (noting that, in cybersecurity and other spheres, although the private sector is subject to some accountability mechanisms, such as market competition, shareholder scrutiny, and disclosure requirements, such industries are not subject to political and public-law accountability mechanisms); *cf.* Jyh-An Lee, *New Perspectives on Public Goods Production: Policy Implications of Open Source Software*, 9 VAND. J. ENT. & TECH. L. 45, 99 (2006) ("[A]s a software consumer, a government is likely to have more concerns than a business consumer does. The difference between a government user and a business user is that, in lending its support to OSS, the government should take into account the long-term interests of society and not merely its own interests as a consumer.").

276. *See, e.g.*, Palmer, *supra* note 4, at 361–62.

277. *See, e.g.*, Etzioni, *supra* note 4, at 96; *see also* Sargsyan, *supra* note 34, at 2223 ("Implementing technical solutions to . . . security issues can increase the cost of conducting business."); Tene, *supra* note 1, at 419 (warning that private sector entities may be tempted to use the information they store for business purposes and eventually harm cybersecurity).

278. Ryan et al., *supra* note 169.

to the domestic market.[279] This anticompetition policy is desirable to China because homegrown technologies are perceived as being more trustworthy than foreign ones, especially in the context of cybersecurity.[280] Dependence on foreign technologies has been viewed as posing a threat to cybersecurity in China.[281] Favoring domestic technology also echoes President Xi Jinping's recent "foreign technology substitution" policy based on "indigenous innovation."[282] These factors may explain why the Chinese government has intervened in the market via the Cybersecurity Law and other regulations. After all, even U.S. cybersecurity expert James A. Lewis believes that "[t]he market has failed to secure cyberspace."[283]

Nevertheless, the government may also fail to achieve its policy goals because of its inability to acquire sufficient information to make decisions.[284] The Cybersecurity Law has given the government the freedom to decide which products and services satisfy cybersecurity requirements and determine the ideal standards on which to base those decisions.[285] However, whether the government has the expertise to make such decisions is unclear.[286] Additionally, the government may not be fully aware of the costs borne by the private sector as a result of the data localization requirement because those costs are not imposed on the government itself. Under the Cybersecurity Law, the government does not need to change its data storage practices because it only stores its data within the territory.[287] By contrast, data localization will be extremely costly for the private sector.[288] This side effect of government intervention is one of the so-called "derived externalities."[289] These potential government failures

279. *See supra* text accompanying note 205; *see also* Iasiello, *supra* note 20 (suggesting that China is "using its strict mandates [in the Cybersecurity Law and other legislation] to protect Chinese businesses from foreign competition").

280. Yuen, *supra* note 61, at 57.

281. *See, e.g.*, Shackelford et al., *supra* note 2, at 32.

282. OFFICE OF THE U.S. TRADE REPRESENTATIVE, *supra* note 169, at 34.

283. Etzioni, *supra* note 4, at 95.

284. *See, e.g.*, Julian Le Grand, *The Theory of Government Failure*, 21 BRIT. J. POL. SCI. 423, 438–39 (1991).

285. Cybersecurity Law, *supra* note 8, art. 23; *id.* art. 35 ("Where the operators of key information infrastructure purchase network products and services that may affect the national security, they shall pass the national security review jointly organized by the State Grid Information Department and the relevant department of the State Council.").

286. *See, e.g.*, Etzioni, *supra* note 4, at 95–96 (suggesting that cybersecurity measures mandated by governments may be cumbersome, inflexible, and inefficient); Palmer, *supra* note 4, at 297–98 (asserting that "the government lacks the understanding to regulate [cybersecurity matters] effectively across so many diverse sectors"); *id.* at 362 (expressing doubt as to whether the government has the expertise to develop cybersecurity standards for a wide range of industries and sectors).

287. *See* Sargsyan, *supra* note 34, at 2231.

288. *See supra* text accompanying notes 163–69.

289. *See* Le Grand, *supra* note 284, at 430.

explain why a poorly crafted cybersecurity regime may run the risk of hindering market efficiency and innovation and even decrease a country's degree of cybersecurity.[290]

In order to ensure cybersecurity, the development of a certification and inspection regime for network products is inevitable in every country. A proposal by the White House provides a plausible alternative to China's government-centric approach to security certification and inspection.[291] In June 2015, the Obama administration announced the #CyberUL initiative to develop a product security standard based on the prominent Underwriters Laboratories ("UL") model that has already been widely adopted in various industries.[292] UL is known for its reliable service in auditing and inspecting products and issuing certificates endorsing its security standard.[293] This approach may not only mitigate the government's weaknesses mentioned above[294] but also alleviate the potential for market failure resulting from private companies' inadequate incentives to acquire products that meet the appropriate cybersecurity standard. Nevertheless, given the lack of a reputable neutral party like UL, and the Chinese government's insistent and strict control over the internet,[295] it is unsurprising that the new law grants the monopoly on conducting security certification, inspection, and review to the government.[296] Although the Chinese government has embarked on an initiative to develop its own standards for cybersecurity, such as the MLPS,[297] whether these standards will effectively help China protect its cybersecurity is presently unclear.

C. Enforcement of Vague Legislation

The Cybersecurity Law has been criticized for being too vague and ambiguous in its language.[298] In fact, using broad and vague language is a feature of most Chinese legislation.[299] Chinese

290. *See, e.g.*, Palmer, *supra* note 4, at 297–98; *cf.* Carter & Sofio, *supra* note 1 ("A poorly crafted cyber regulatory regime could end up constraining the private sector and making U.S. critical infrastructure networks less secure and making U.S. critical companies less nimble in securing their network.").

291. *See supra* Subpart III.D.

292. Carter & Sofio, *supra* note 1, at 238.

293. *Id.*

294. *See* Sargsyan, *supra* note 34, at 2223–24.

295. *See, e.g.*, Yuen, *supra* note 61, at 53 ("China has . . . been known for its highly restrictive Internet control.").

296. *See id.* at 54.

297. *See supra* text accompanying note 185.

298. *See supra* text accompanying notes 20–26, 90, 123–28, 139–40, 197–98.

299. *See, e.g.*, Christopher Duncan, *Out of Conformity: China's Capacity to implement World Trade Organization Dispute Settlement Body Decisions after Accession*, 18 AM. U. INT'L L. REV. 399, 412, 418–19 (2002); Parasol, *supra* note 60, at 87; Randall Peerenboom, *The X-Files: Past and Present Portrayals of China's Alien "Legal System,"* 2 WASH. U. GLOBAL STUD. L. REV. 37, 81 (2003); Leontine D. Chuang, Comment, *Investing in China's Telecommunications*

legislation typically provides an administrative body with significant flexibility to interpret and enforce the law.[300] Such flexibility is intentional to allow for response to rapid social and economic changes.[301] In order to enforce the law, regulatory and administrative agencies need to create more detailed administrative rules.[302] However, the downside of this approach is that Chinese law is consequentially inconsistent and arbitrary.[303] This weak rule-of-law regime has created significant uncertainties and transaction costs for business operations.[304] Such shortcomings certainly also appear in the Cybersecurity Law.

The vagueness of the language used in the Cybersecurity Law implies that the government may intend to use it as a tool to control industries. Some commentators believe that, similar to many other laws and regulations in China, the vague Cybersecurity Law was designed to give the authorities more flexibility and leeway to interpret and implement it.[305] For example, the authorities in charge may apply a case-by-case approach to interpreting the law.[306] The worst-case scenario would be that the law is enforced to engage in selective persecution. Regulators may harshly enforce the law against disobedient people or companies who have become a thorn in the side of the nation-state.[307] Therefore, a more fundamental concern in terms of the new law is probably not the vagueness of its language but, rather, the fact that the country has few democratic checks and balances.[308] That creates an enormous gray area for law enforcement.

Given the Cybersecurity Law's ambiguity, it will take time for internet companies to observe and begin to understand how the government intends to enforce the law. The real impact of the law then depends on how regulators interpret it.[309] Although, from the

---

Market: Reflections on the Rule of Law and Foreign Investment in China, 20 NW. J. INT'L L. & BUS. 509, 525 (2000); Meixian Li, Comment, *China's Compliance with WTO Requirements Will Improve the Efficiency and Effective Implementation of Environmental Laws in China*, 18 TEMP. INT'L & COMP. L.J. 155, 165 (2004); Lindsay Wilson, Note, *Investors Beware: The WTO Will Not Cure All Ills with China*, 2003 COLUM. BUS. L. REV. 1007, 1017 (2003).

300. Duncan, *supra* note 299, at 419; Li, *supra* note 299.

301. *See, e.g.*, Ruth Jebe et al., *China's Export Restrictions of Raw Materials and Rare Earths: A New Balance Between Free Trade and Environmental Protection?*, 44 GEO. WASH. INT'L L. REV. 579, 630 (2012).

302. *See id.*

303. *See id.*; Li, *supra* note 299, at 166.

304. *See* Akerman et al., *supra* note 181; *cf.* Chuang, *supra* note 299, at 510 ("[T]he vague legal framework for foreign investment in China can make investment in China an unpredictable venture.").

305. Clover & Ju, *supra* note 15.

306. *See* Iasiello, *supra* note 20.

307. *See id.*

308. *See id.* at 5 (noting that the group overseeing Chinese internet security "will have complete authority over online activities").

309. *See, e.g.*, Clover & Ju, *supra* note 15.

private sector's perspective, a strict interpretation will make it impossible to entirely comply with the law, from the regulators' perspective, it is also impossible to enforce the law in a comprehensive way across different industries given the government's limited resources.[310] The broad language used in the Cybersecurity Law may also be relevant to the pervasive nature of digital networks, which has made it impossible for the government to respond to all sorts of threats with finite resources.[311] Therefore, given the vagueness mentioned above, the government needs to consider a wide range of circumstances and set priorities in its enforcement of the Cybersecurity Law.

D. Digital Human Rights with Chinese Characteristics

Cybersecurity concerns some fundamental human rights. Consequently, scholars have proposed that human rights implications should be included in the cybersecurity dialogue between China and the United States.[312] China is notorious for its human rights violations.[313] However, it would be naïve to argue that it does not protect human rights at all. Domestically, human rights have been entrenched in China's constitution since 1982.[314] In 2004, the constitution was amended to provide expressly that "the state respects and [safeguards] human rights."[315] Internationally, China voted together with the United States in favor of the 2012 United Nations Human Rights Council resolution to protect the free speech of individuals on the internet, which directly addressed the right to freedom of expression and opinion on the internet.[316] Although China has made some progress in its human rights protections, its approaches to human rights have reflected values and mentalities

310. *See supra* text accompanying notes 284–90.

311. Carter & Sofio, *supra* note 1.

312. *See, e.g.*, Lewis, *supra* note 46, at 492.

313. *See, e.g.*, Chow, *supra* note 77, at 682; Lawrence Friedman, *On Human Rights, the United States and the People's Republic of China at Century's End*, 4 J. INT'L LEGAL STUD. 241, 241, 249–50 (1998); Fry, *supra* note 211, at 420; Lewis, *supra* note 46, at 472, 484–88; Peerenboom, *supra* note 77, at 72; Zhang, *supra* note 77, at 263–64.

314. *See* XIANFA arts. 33–56 (1982) (China); *see also* PERRY & RODA, *supra* note 61 ("The 1982 Chinese Constitution guarantees freedom of speech, publication, assembly, association, precession, and demonstration under article 35.").

315. XIANFA art. 33 (1982) (China).

316. *See* Wendy Zeldin, *U.N. Human Rights Council: First Resolution on Internet Free Speech*, LIBR. CONG. (July 12, 2012), http://www.loc.gov/law/foreign-news/article/u-n-human-rights-council-first-resolution-on-internet-free-speech/. *But see* CHANDER, *supra* note 74, at 202 (noting that, although China has signed the International Covenant on Civil and Political Rights, another important international document regarding the protection of human rights, the country has not yet ratified the treaty).

that are rather different from those of the Western world.[317] This is why the Chinese government has claimed that "no country in its effort to realize and protect human rights can take a route that is divorced from its history and its economic, political and cultural realities."[318]

China's human rights philosophy is reflected in its approach to internet governance, which has been largely state-centric and accentuates individual responsibilities over individual rights.[319] China's Cybersecurity Law and its cybersecurity policies have provided a lens through which to understand the status quo in terms of the country's perspectives on human rights. Take privacy or protection of personal information as examples. As mentioned previously, although the law provides citizens with unprecedented protection of their data privacy, it also creates numerous opportunities for the government or third parties to infringe upon citizens' privacy.[320] Why does the law take such a seemly inconsistent or parallel approach to privacy by protecting and risking privacy simultaneously? This Article argues this occurrence can be explained by the fact that the fundamentals of China's human rights are different from those of the Western world. In the Western world, human rights were designed to protect individuals from state power since the beginning.[321] However, China has viewed human rights as derived from the state, which reigns supreme over the individual.[322] Therefore, human rights are never considered to represent an individual's rights over those of the Chinese state.

By this logic, it is not difficult to understand why, under the Cybersecurity Law, network operators are obliged to provide

317. *Cf.* Jiang, *supra* note 59, at 81 (arguing that China "is promoting good governance and defining democracy in its own terms, although not in the liberal democratic sense").

318. *See* MINISTRY OF FOREIGN AFFAIRS OF CHINA, HUMAN RIGHTS IN CHINA, at pt. X (2002), http://www.fmprc.gov.cn/mfa_eng/topics_665678/3711_665954/t18997.shtml#10.

319. Jiang, *supra* note 59, at 73.

320. *See supra* Subpart III.E; *see also In China, Consumers Are Becoming More Anxious About Data Privacy: Will This Impede the Government's Snooping?*, ECONOMIST (Jan. 25, 2018), https://www.economist.com/news/china/21735613-will-impede-governments-snooping-china-consumers-are-becoming-more-anxious-about-data (detailing the government's campaign of "examining the privacy policies of [] internet firms" and asserting that "the public's growing concerns about privacy must be at odds with the government's efforts to create a new form of surveillance state"); Merrion, *supra* note 16 (noting that the law "creates broad privacy protections, but it also requires users to be identified by their real names . . . and it requires network operators to provide 'technical support and assistance' to government investigators").

321. *See, e.g.*, Chow, *supra* note 77, at 688–89; Alon Harel, *How (and Whether) to Rethink Human Rights*, 9 INT'L LEGAL THEORY 87, 90–91 (2003); Michael J. Perry, *Protecting Human Rights in A Democracy: What Role for the Courts?*, 38 WAKE FOREST L. REV. 635, 636, 644 (2003); Steven R. Ratner, *Corporations and Human Rights: A Theory of Legal Responsibility*, 111 YALE L.J. 443, 469 (2001).

322. *See* Chow, *supra* note 77, at 692–93.

individuals with an impressive degree of privacy,[323] yet individuals cannot claim any remedies for the infringements of their privacy carried out by the state government. Similarly, China has developed an increasingly sophisticated approach to free speech, taking into account the free flow of information, an individual's reputation, privacy, and the nature of social media.[324] Nevertheless, political speech against the government is still highly controlled,[325] and the exercise of human rights is not permitted to threaten the regime or social stability.[326] While the government has endeavored to continuously enhance the human rights protection it offers, the actions of the state government itself is mostly unconstrained by fundamental human rights.[327]

Human rights philosophy has also influenced the structure and function of the Chinese government. In Western democracies, human rights protection is ensured through checks and balances.[328] This checks-and-balances mechanism plays a critical role in balancing national security with human rights.[329] Comparatively, while government surveillance for law enforcement or national security purposes is also common in other jurisdictions, the implementation of such surveillance is usually subject to various levels of scrutiny in order to balance different interests, especially those concerning criminal investigations, national security, privacy, and civic

323. *See supra* text accompanying notes 215–21.

324. *See* Jyh-An Lee, *Regulating Blogging and Microblogging in China*, 91 OR. L. REV. 609, 616–20 (2012); *see also* Jiang, *supra* note 59, at 73 (documenting Beijing's assurances to its citizens regarding freedom of speech).

325. *See, e.g.*, Jiang, *supra* note 59, at 73–74; Lee, *supra* note 324, at 612–14.

326. *See, e.g.*, Peerenboom, *supra* note 77, at 97.

327. *See, e.g.*, *id.* at 106 ("Although the media regularly carries exposés on corruption, the government has imposed limits on stories involving high-level officials, for which approval must be obtained.").

328. *See, e.g.*, Benedikt Goderis & Mila Versteeg, *Human Rights Violations After 9/11 and the Role of Constitutional Constraints*, 41 J. LEGAL STUD. 131, 132 (2012); Mireille Hildebrandt, *The Trial of the Expert: Épreuve and Preuve*, 10 NEW CRIM. L. REV. 78, 92–93 (2007); Waikeung Tam, *Political Transition and the Rise of Cause Lawyering: The Case of Hong Kong*, 35 LAW & SOC. INQUIRY 663, 681 (2010); *see also* Maria Dakolias, *Are We There Yet?: Measuring Success of Constitutional Reform*, 39 VAND. J. TRANSNAT'L L. 1117, 1134–35 (2006) (noting that the extent to which "checks and balances protect individuals from state power" serves as a proxy by which to measure the quality of constitutional governance).

329. *See, e.g.*, Amos N. Guiora, *Human Rights and Counterterrorism: A Contradiction or Necessary Bedfellows?*, 46 GA. L. REV. 743, 745–46 (2012); Lucas Guttentag, *Immigrants' Rights in the Courts and Congress: Constitutional Protections and the Rule of Law After 9/11*, 25 WASH. U. J.L. & POL'Y 11, 24 (2007); Harold Hongju Koh, *Can the President Be Torturer in Chief?*, 81 IND. L.J. 1145, 1155 (2006); C. Raj Kumar, *Human Rights Implications of National Security Laws in India: Combating Terrorism While Preserving Civil Liberties*, 33 DENV. J. INT'L L. & POL'Y 195, 197 (2005); Anne-Marie Slaughter & William Burke-White, *The Future of International Law Is Domestic (or, The European Way of Law)*, 47 HARV. INT'L L.J. 327, 348 (2006).

liberties.[330] For example, in the United States, the Foreign Intelligence Surveillance Act restricts the government's authority to use electronic surveillance inside the United States to obtain foreign intelligence and requires the government to obtain a warrant or court order from the Foreign Intelligence Surveillance Court to engage in certain foreign intelligence activities.[331] By contrast, since China has neither effective checks and balances nor judicial independence,[332] the courts play no role in ensuring that the administrative authorities will not abuse their power and infringe upon a person's humans rights for the purposes of protecting national security. As a result, the Cybersecurity Law provides various provisions that enable the government's surveillance and control over information without substantial constraint.[333]

Apple's dispute with the Federal Bureau of Investigation ("FBI") in the United States also provides a good example illustrating the differences in the human rights philosophy promoted by the Western world in comparison to that of China. In February 2016, the FBI asked Apple to unlock an iPhone belonging to one of the accused killers in a mass shooting event that took place in San Bernardino, California, but Apple refused the request.[334] The Department of Justice obtained a court order mandating that Apple decrypt the iPhone.[335] Apple challenged the order,[336] and on March 28, 2016—the eve of a hearing—the government announced that the FBI had successfully unlocked the iPhone with the assistance of a third

330. *See, e.g.*, United States v. U.S. District Court (*Keith*), 407 U.S. 297, 322–23 (1972); Katz v. United States, 389 U.S. 347, 347 (1967); United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980).

331. *See* 50 U.S.C. § 1801(a)–(f) (2012); Fry, *supra* note 211, at 454.

332. *See, e.g.*, Paul H. Anderson, *A Minnesota Judge's Perspective on the Rule of Law in China and Kyrgyzstan*, 18 MINN. J. INT'L L. 343, 349 (2009); Ann Bartow, *Privacy Laws and Privacy Levers: Online Surveillance Versus Economic Development in the People's Republic of China*, 74 OHIO ST. L.J. 853, 861 (2013); Ji Weidong, *The Judicial Reform in China: The Status Quo and Future Directions*, 20 IND. J. GLOBAL LEGAL STUD. 185, 195 (2013); Alex L. Wang, *Regulating Domestic Carbon Outsourcing: The Case of China and Climate Change*, 61 UCLA L. REV. 2018, 2054 (2014).

333. *See, e.g.*, *supra* text accompanying notes 176, 201–03.

334. Hurwitz, *supra* note 101, at 403; Tracey Lien et al., *Court Order in San Bernardino Case Could Force Apple to Jeopardize Phone Security*, L.A. TIMES (Feb. 17, 2016, 1:54 PM), http://www.latimes.com/local/lanow/la-me-ln-apple-san-bernardino-security-20160217-story.html; Danny Yadron et al., *Inside the FBI's Encryption Battle with Apple*, GUARDIAN (Feb. 18, 2016, 1:00 AM), https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple.

335. Eichensehr, *supra* note 275, at 487.

336. *Id.*

party,[337] ending the lawsuit between Apple and the government.[338] Conversely, no such restriction exists under the Cybersecurity Law to constrain the government's power to demand decryption assistance. The Chinese government can request that companies provide access to personal information or decryption assistance to access such information without the need for a court order.[339] In sum, the Cybersecurity Law perpetuates China's human rights practice of prioritizing government supremacy.

V. CONCLUSION

The Cybersecurity Law is a milestone in China's laws and policies regarding the internet. The law not only reflects China's increasingly strict governance of the internet but also reveals China's attempts to assert its internet sovereignty and shows that the country is taking cybersecurity issues more seriously now than ever. The law reaffirms China's intention to dictate the regulation of its own cyberspace and provides the government with the legal facades with which to identify and mitigate the online behaviors that it deems unacceptable. While it is common for governments to impose restrictions on the private sector when there are cybersecurity concerns, China has decided to take a more militant and draconian approach than most other countries.

Under the new Cybersecurity Law, network operators—especially those in the category of critical information infrastructure operators—are burdened with hefty legal obligations to protect cybersecurity.[340] Different from the United States' voluntary policy, the Cybersecurity Law adopts a mandatory approach to protect critical infrastructure.[341] Both voluntary and mandatory approaches have their respective advantages and disadvantages. China's Cybersecurity Law will test whether the mandatory approach is effective and sustainable in terms of protecting critical infrastructure. Data localization is one of the most cumbersome duties borne by critical information infrastructure operators, and it is unclear whether such data localization can adequately protect cybersecurity in the long run. However, the data localization policy does expose enterprises to more risks associated with local government

337. Hurwitz, *supra* note 101, at 404; Arjun Kharpal, *Apple vs FBI: All You Need to Know*, CNBC (Mar. 29, 2016, 6:34 AM), https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html; Kim Zetter, *The FBI Drops Its Case Against Apple After Finding a Way into that iPhone*, WIRED (Mar. 28, 2016, 6:18 PM), https://www.wired.com/2016/03/fbi-drops-case-apple-finding-way-iphone/.

338. Danny Yadron, *San Bernardino iPhone: US Ends Apple Case After Accessing Data Without Assistance*, GUARDIAN (Mar. 29, 2016, 2:24 AM), https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone.

339. *See supra* text accompanying notes 100–103.

340. Cybersecurity Law, *supra* note 8, art. 21.

341. *Id.* art. 9.

surveillance. Although its protection of citizens' data privacy is unprecedented, the Cybersecurity Law also grants the government significant power to access personal information which could possibly be leaked.

This Article argues that the Cybersecurity Law should be understood from the perspective of China's unique conception of cybersecurity, which is much broader than the Western world's definition. In China, cybersecurity encompasses content control for the purposes of maintaining social and political stability. Furthermore, the Cybersecurity Law's treatment of personal information and privacy mirrors China's perceptions of human rights: human rights are protected under the law, but they must yield to government power. Government supremacy is an essential part of Chinese human rights philosophy. This explains why the Cybersecurity Law extends an unprecedented level of protection to privacy while also providing the government with unparalleled power to control and surveil the personal information held by various network operators.