Santa Clara Law Review

Volume 58 | Number 1 Article 4

6-4-2018

China's New Cybersecurity Law and U.S-China Cybersecurity Issues

Liudmyla Balke

CHINA'S NEW CYBERSECURITY LAW AND U.S.-CHINA CYBERSECURITY ISSUES

Liudmyla Balke*

TABLE OF CONTENTS

* M.A. Zaporizhzhya Institute of State and Municipal Management, Ukraine, J.D. Santa Clara University School of Law. Getting certified an as information privacy professional prompted my research on the cyber security issues. I want to thank Professor Anna Han of Santa Clara Law School for providing me with an invaluable insight into the Chinese history and culture that helped in writing of this comment. I am also appreciative of my family, friends, and fellow Santa Clara Law Review board members that helped along the way.

INTRODUCTION

"Cyberspace." It is difficult to define, notwithstanding its ubiquitous nature, perhaps because of its mutable characteristics.[1] At the same time, cyberspace makes the Internet unique as "an inherently borderless medium of communication."[2] The Internet has undeniably become a global digital phenomenon.

Trying to define cyberspace in clear terms is challenging. One court defined it as a "world of electronic communications over computer networks."[3] Scholars prefer a more complex definition, referring to a cyberspace as an "evolving man-made domain for the organization and transfer of data . . . a combination of private and public property governed by technical rule sets designed primarily to facilitate the flow of information."[4]

Cyberspace is consistently growing, with at times unidentifiable interconnections, most of it in the private sector.[5] Thus, establishing a national framework for cybersecurity is no easy task.[6] A coherent framework, however, is necessary[7] and important, as "thousands of interconnected computers, servers, routers, switches and fiber optic cables" that comprise cyberspace are crucial for the proper functioning of critical infrastructures.[8] Cyberattacks can instantaneously cross international borders through cyberspace, implicating computers in countries long distances apart.[9] A more defined structure would make it

---

1. *See* Lance Strate, *The Varieties of Cyberspace: Problems in Definition and Delimitation*, 63 W. J. OF COMM. 382, 382–83 (1999).

2. Susanna Bagdasarova, *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance*, 119 PENN. ST. L. REV. 1005, 1012 (2015) (citing Jessica E. Bauml, *It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship*, 63 FED. COMM. L.J. 697, 703 (2011)).

3. *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 907 F. Supp. 1361, 1365 n.1 (N.D. Cal. 1995).

4. Bagdasarova, *supra* note 2, at 1010–11 (quoting Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 68 (2009)).

5. ERIC A. FISHER, CONG. RESEARCH SERV., RL32777, CREATING A NATIONAL FRAMEWORK FOR CYBERSECURITY: AN ANALYSIS OF ISSUES AND OPTIONS 6 (2005), https://fas.org/sgp/crs/natsec/RL32777.pdf.

6. *See id.*

7. THE WHITE HOUSE, NATIONAL STRATEGY TO SECURE CYBERSPACE vii (Feb. 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

8. *Id.* at vii.

9. Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, N.Y. TIMES (May 29, 2007), http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (in the April 2007 cyber attack on Estonia's networks, a network of bots located as far away as Vietnam or the United States were used to increase the assault's impact).

easier to react to such unusual circumstances.[10]

Security risks have grown exponentially with the use of the Internet and data storage systems.[11] Cybercrime is now abundant in cyberspace, harming the world's economy and costing billions of dollars in damages.[12] In response to cyber threats, the international community has responded with an array of solutions, including international conventions, national strategies, agreements, summits, and organizations.[13] Unfortunately, all of them lack coherent and mutual structure.

China, the second largest economy in the world, has the most Internet users.[14] It is an undeniably important participant in the global cyber community. The country represents nearly twenty-two percent of total users with more than the United States of America, India, and Japan combined.[15] As of 2017, the United States had over a quarter-billion of the world's Internet users, and is now third only behind China and India.[16] Therefore, the strategies and cybersecurity regulations of China and the United States can provide necessary insights into the nature of cybersecurity policies in general. They also reveal flaws in an area so important to the world's economic development and international cooperation.

Chinese views on cybersecurity and threats of terrorism provide us with some helpful insights.[17] The outward unanimous support of China's official goal of cyber sovereignty suggests that a change in their current position is unlikely.[18] Thus, the People's Republic of China (the PRC)

---

10. FISHER, *supra* note 5 at 6–7.

11. *Id.* at 8.

12. *Id.* at 13; Jeff Kosseff, *The Cybersecurity Privilege*, 12 I/S: J.L. & POL'Y FOR INFO. SOC'Y 261 (2016); Emmanuel Darmois & Geneviève Schméder, *Cybersecurity: A Case for a European Approach*, 7 (2016), http://www.securityintransition.org/wp-content/uploads/2016/02/WP11_Cybersecurity_FinalEditedVersion.pdf.

13. William M. Stahl, Note, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, 40 GA. J. INT'L & COMP. L. 247, 263–65 (2011).

14. *Internet Users by Country*, INTERNETLIVESTATS.COM (last visited Jan. 13, 2017), http://www.internetlivestats.com/internet-users/.

15. *Id.*

16. *Top 20 Countries with the Highest Number of Internet Users*, INTERNETWORLDSTATS.COM (June 30, 2017), http://www.internetworldstats.com/top20.htm.

17. Michael D. Swaine, *Chinese Views on Cybersecurity in Foreign Relations*, China Leadership Monitor no. 42, Oct. 7, 2013, at 16, http://carnegieendowment.org/files/CLM42MS_092013Carnegie.pdf.

18. *Id.*; "China is a high context society in which most people share a common set of norms, values, and beliefs." DANIEL C.K. CHOW & ANNA M. HAN, DOING BUSINESS IN CHINA: PROBLEMS, CASES, AND MATERIALS 63 (2012).

will likely continue to improve their cyber capabilities for both national security and economic purposes.[19]

This comment talks about the tension between the United States and China over cybersecurity and its impact on international trade.[20] The comment then discusses the most pressing concerns resulting from China's new controversial Cybersecurity Law (the CSL), enacted on November 7, 2016.[21] Finally, this comment proposes for global powers like China and the United States, to adopt an integrated European Union (the EU) style approach to cyber security, which rejects "technological determinism and mass surveillance."[22]

II. BACKGROUND

A. Cybersecurity tensions between the U.S. and China

The USA National Institute of Standards and Technology (NIST) provides a useful definition of cybersecurity: "[t]he ability to protect or defend the use of cyberspace from cyber attacks."[23] The world's two major powers, the United States of America and China are both equipped for aggressive cyber-war.[24] Such power comes with enormous responsibilities.

Thus, it is important to distinguish who is using cyber warfare capabilities and for what purposes.[25] Does the country use its abilities to push political agendas against civil societies?[26] Does the country have a genuine policy of using its cyber skills to defend its citizens?[27] Or, more realistically, does it employ both strategies? Both the United States and China are known for their use of cyber security "in the name of the fight against terrorism."[28] However, the Snowden revelations brought the degree of U.S. secret illegal cyberspace operations to light.[29] To which

19. Swaine, *supra* note 17, at 16.

20. *See infra* Part II.A.

21. *See infra* Part IV.

22. Darmois & Schmeder, *supra* note 12, at 5; *see infra* Part V.

23. Darmois & Schmeder, *supra* note 12, at 5 (citing Richard Kissel, *Glossary of Key Information Security Terms*, 58 (May 2013), http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

24. *See id.*; *see also* John R. Lindsey, *Inflated Cybersecurity Threat Escalates US-China Mistrust*, HUFFPOST (last visited Feb. 17, 2018) https://www.huffingtonpost.com/jon-r-lindsay/cybersecurity-threat-escalates-us-china-mistrust_b_7302282.html.

25. Darmois & Schmeder, *supra* note 12, at 9.

26. *Id.*

27. *Id.*

28. *Id.* at 10.

29. Ewen Macaskill & Gabriel Dance, *NSA Files: Decoded*, THE GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-

the global community questioned U.S. compliance with democratic principles.[30]

The revelations showed that the National Security Agency targeted not only other countries, but also ordinary citizens, making the life of active participants in civil society more difficult.[31] The United States' use of counter-technology is an example of the blurred lines between the government's goal of preventing terrorist attacks and public use of protective technologies.[32] Likewise, in China, the true motives behind cybersecurity regulations are often unclear.

The views on cybersecurity between the United States and China differ starting at the basic ideological level. From an American perspective, the ideal Internet is an open, secure platform, free for all to enjoy.[33] The Chinese start from a completely different position.[34] The Chinese government decided a long time ago that it wants to be in "control of the narrative about . . . China's rise."[35] China wants to be completely independent from other countries, which largely prompted the idea of cyber sovereignty within the country.

Independence, innovation, and inner prosperity push the Chinese government to do so.[36] Wariness of the technology trap and a desire to transcend their manufacturing economy motivates China's impatience and enormous investment in Research and Development.[37] An ambition for self-sufficiency[38] also explains China's alleged hacking, spying, and stealing of important corporate data by the PRC intelligence.[39]

The Snowden revelations put the United States in an interesting position, to say the least.[40] China had always assumed that the United States was hacking into their networks even before the revelations.[41] The NSA and other government agencies were, in fact, breaking into Chinese

---

surveillance-revelations-decoded#section/1.

30. Darmois & Schmeder, *supra* note 12, at 10.

31. *Id.*

32. *Id.*

33. The Christian Science Monitor, *Cybersecurity from China's Perspective,* YOUTUBE (Feb. 4, 2016), https://www.youtube.com/watch?v=XINwf7xj5to&t=292s [hereinafter Science Monitor].

34. *Id.*

35. *Id.*

36. *Id.*

37. *Id.*; *see generally* Justin Yifu Lin, *Economic Growth and Development*, *in* ROUTLEDGE HANDBOOK OF THE CHINESE ECONOMY 76–89 (Gregory C. Chow & Dwight H. Perkins eds., 2015) (describing the reasons for and costs of China's transition to a dynamic economy).

38. CHOW & HAN, *supra* note 18, at 15.

39. *See* Science Monitor, *supra* note 33.

40. *See generally* Macaskill, *supra* note 29.

41. *See* Science Monitor, *supra* note 33.

networks in search of political and military secrets.[42] Curiously, the U.S. government differentiates between good hacking and bad hacking, with political espionage considered good.[43] Bad hacking, accordingly, occurs when, for instance, the Chinese allegedly hack into a foreign company's network to steal intellectual property to help domestic private and state owned companies become more competitive and independent.[44]

As a dim glimmer of hope, the two countries have finally tried to work out some of the pressing cybersecurity issues. In 2015, President of China, Xi Jinping, while visiting the U.S., signed a cyber agreement that prohibits both countries from knowingly supporting cyber theft of intellectual property for the economic advantage of domestic companies.[45] The 2015 visit was a success, considering that just two years prior, at a summit in California, the two presidents could not reach any consensus on cybersecurity.[46]

China's alleged cyber attacks have worried both the United States and the international community for quite some time.[47] The Wall Street

---

42. *Id.*

43. *Id.*

44. *Id.*

45. *See* John W. Rollins, *U.S.–China Cyber Agreement*, CRS INSIGHT (Oct. 16, 2015), https://fas.org/sgp/crs/row/IN10376.pdf; *accord* Julie Hirshfield Davis & David E. Sanger, *Obama and Xi Jinping of China Agree to Take Steps on Cybertheft*, N.Y. TIMES (Sept. 25, 2015), http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html; *accord* Demetri Sevastopulo & Geoff Dyer, *Obama and Xi in deal on cyber espionage*, FINANCIAL TIMES (Sept. 25, 2015), https://www.ft.com/content/0dbcab36-63be-11e5-a28b-50226830d644.

46. *Compare* Gary Brown & Christopher D. Yung, *Evaluating the US-China Cybersecurity Agreement*, THE DIPLOMAT (Jan. 19, 2017), https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/ (supporting the claim that a first agreement of its kind, reached during the 2015 Chinese President's United States visit, was a positive step), *with* SCOTT WARREN HARROLD ET AL., GETTING TO YES WITH CHINA IN CYBERSPACE 10 (2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf (concluding that the results of the 2013 summit were exiguous because of China's denial of cyber espionage); *and* Charles Riley, *Obama and Xi fail to bridge cybersecurity gap*, CNN MONEY U.S. (June 10, 2013, 5:38 AM), http://money.cnn.com/2013/06/10/news/obama-china-cybersecurity ("no firm commitments on cyber-related issues were secured at the conference").

47. *See* Magnus Hjortdal, *China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence*, 4 J. OF STRATEGIC SECURITY 6 (2011), http://scholarcommons.usf.edu/jss/vol4/iss2/2 (last visited Dec 28, 2016); *see also* Eric Talbot Jensen, *Cyber Deterrence*, 26 Emory Int'l L. Rev. 733, 784–86 (2012) (citing *China, Not India, Behind Cyber Attacks*: *US*, HINDUSTAN TIMES (India) (Jan. 21, 2012), http://www.hindustantimes.com/world-news/Europe/China-not-India-behind-cyber-attack-US/Article1 -800051.aspx, *and* Charles Arthur, *China 'Targeted 48 Chemical and Military Companies in Hacking Attack*, GUARDIAN (Nov. 1, 2011), http://www. guardian. co.uk/technology/2011 /nov/01 /china-hacking-chemical- military-companies) (naming several instances of cyber-attacks linked to China but disguised as coming from other sources); for a discussion of China's harmful cyber attacks

Journal (the WSJ) in its article on the world's cyber forces stated that China "[o]ften uses high-volume attacks with a large number of operatives in military or outside groups linked to [the] government who bombard targets."[48] According to the WSJ, a list of suspected acts by the Chinese in recent years includes:

> 2009: Theft of data from Google Inc. and other tech companies.
> 2009: Discovery of theft of plans for U.S. Joint Strike Fighter project.
> 2010: Attacks on British executives.
> 2011: Attack on South Korean Internet portal.
> 2013: Major U.S. media companies hacked.
> 2015: "Great Cannon" directs massive amounts of traffic to take anticensorship websites offline.
> 2015: Hack of U.S. Office of Personnel Management.[49]

Particularly, China has often been a suspect of industrial espionage aimed at increasing its competitiveness globally.[50]

Although, the United States is no innocent bystander when it comes to hacking.[51] The WSJ talks about the United States' cyber warfare capabilities, as headed by the NSA and Cyber Command.[52] The United States' attacks are known for their complexity and sophisticated techniques, as the country has been active in the field for nearly two decades.[53] The list of suspected acts includes:

> 2010: Discovery of computer worm that destroyed centrifuges at
> Iranian nuclear plant.
> 2010: Surveillance of EU offices.
> 2011: Attack on Gemalto, a European maker of mobile SIM cards,

---

against the United States see Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 Eur. J. Int'l L. 129, 131 (2013).

48. Jenifer Valentino-Devries & Danny Yadron, *Cataloging the World's Cyberforces,* THE WALL STREET JOURNAL (Oct. 11, 2015, 8:45 PM) http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

49. *See id.* (Hydraq, which was found in Google attack and others, and Sakula, which was found in OPM attack and others, were identified as malware used in those attacks).

50. RICHARD STIENNON, SURVIVING CYBERWAR 49, 15 (2010); Gordon G. Chang, *Obama's Summit with Xi Jingping: Where's the Tough Love?*, THE DAILY BEAST (Jun. 9, 2013, 4:45 AM), http:// www.thedailybeast.com/articles/2013/06/09/obama-s-summit-with-xi-jinping-where-s-the-tough-love.html (according to some of the estimates by government officials, intellectual property theft, ascribed to alleged Chinese hackers, causes U.S. companies to lose $250 billion each year).

51. Jyh-An Lee, *The Red Storm in Uncharted Waters: China and International Cyber Security*, 82 UMKC L. Rev. 951, 953 (2014).

52. *See* Valentino-Devries & Yadron, *supra* note 48.

53. *See id.*

likely with Britain's GCHQ."[54]

Flame, a type of espionage malware; Stuxnet, used in the Iranian attack; and GrayFish, a high-level malware able to attack computer "firmware" at the heart of the computer's hard drive and resurrect itself, are only some used by the US intelligence.[55]

Considering that the PRC has impressive capabilities of aggressive cyber-intrusion, nations cannot simply ignore the possible threat of cyber attacks on their networks.[56] In addition to targeting governments, the alleged Chinese attackers infiltrate private sector companies.[57] Some American enterprises, which have become victims of cyber attacks in the recent years, include Apple, Facebook, Google, Twitter, and *the Washington Post*.[58]

As mentioned earlier, China sees itself not as an initiator, but rather a victim of the cyber attacks, often condemning similar hacking by the United States of Chinese computer systems.[59] And in fact, the modernization of Chinese cyber weapons and improvement of its hacking abilities is prescribed due to "pressures caused by American technological power."[60]

On an optimistic note, both powers have shown initiative and willingness to engage in the common resolution of cybersecurity issues.[61] As both the U.S. and China understand that setting international rules for cybersecurity is important, they seem to be willing to cooperate.[62]

---

54. *Id.*

55. *Id.; see also* Lee, *supra* note 51, at 953 (citing Ron Rosenbaum, *Richard Clarke on Who Was Behind the Stuxnet Attack*, SMITHSONIAN MAGAZINE (Apr. 2012), http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html).

56. *See* Hjortdal, *supra* note 47, at 6 (citing *China: Pushing Ahead of the Cyberwarfare Pack,* STRATFOR (Mar. 2, 2009, 3:27 PM), https://worldview.stratfor.com/article/china-pushing-ahead-cyberwarfare-pack) ("Analysts say that China could well have the most extensive and aggressive cyber warfare capability in the world.").

57. Lee, *supra* note 51, at 954.

58. Stephen Moore, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 N.C.J. Int'l L. & Com. Reg. 223, 253 (2014); Riley, *supra* note 46.

59. Lee, *supra* note 51, at 957–58.

60. *Id.* at 958.

61. Lee, *supra* note 51, at 958.

62. *See id.* at 958. For a statement by Chinese Premier Li Keqiang on the need to make fewer accusations and contribute more to cybersecurity, see Terril Yue Jones and Benjamin Kang Lim, *China's New Premier Seeks "New Type" of Ties with U.S.*, REUTERS(Mar. 17, 2013, 4:02 AM), https://www.reuters.com/article/us-china-parliament-hacking/chinas-new-premier-seeks-new-type-of-ties-with-u-s-idUSBRE92G02320130317.

1. Cultural factors, which impacted China's new Cybersecurity Law.

The PRC has been a state-controlled economy since its founding in 1948 until 1978 when economic reforms took place.[63] The state controlled capital apportionment for investment in business enterprises.[64] Banks mostly lent money to enterprises not to increase productivity, but rather for political reasons.[65] The apparent preference, given to domestic companies in China, also dates back to the emphasis of state-owned enterprises (SOEs) as "essential units of the state and the foundation of the economy."[66]

During the 1949–1978 period, China did not engage in foreign trade with other nations with a few slight exceptions.[67] The country's focus was mainly inward.[68] This isolationism, typical of the present day economic policies, developed because foreign imperial powers dominated the country from 1850 to 1949 and suppressed China's power.[69]

Because of the political chaos and unwise economic policies, before the economic reforms were promulgated in 1978, China's economy suffered from stagnation, inefficiency, and almost no economic growth.[70]

Considering such a turbulent history and weak economic state, China's transition to one of the fastest growing economies in only three decades is noteworthy.[71] However, with a population of approximately 1.331 billion and a Gross Domestic Product of $5.11 trillion in 2009,[72] China is still a developing country.[73] China remains a comparatively poor country in general, and ranks as one of the world's lowest-income

63. CHOW & HAN, *supra* note 18, at 12.

64. *Id.* at 14 (In the US, by contrast, capital is allocated to enterprises through different market mechanisms, like the sale of stocks or bonds, venture capital borrowing and reinvestment of excess earnings).

65. *Id.*

66. *Id.*

67. CHOW & HAN, *supra* note 18, at 15.

68. *Id.*

69. *Id.*

70. *Id.* at 16–17.

71. CHOW & HAN, *supra* note 18, at 19 (with nearly 10 percent growth rate on average, such dramatic improvement is unprecedented).

72. The World Bank, China, http://data.worldbank.org/country/china (last visited Jan. 3, 2018).

73. Bauml, *supra* note 2, at 724 (citing International Monetary Fund, *Restoring Confidence Without Harming Recovery* 2, tbl.1 (July 7, 2010), http:// www.imf.org/external/ pubs/ft/weo/2010/update/02/pdf/0710.pdf).

countries.[74] It is a nation still in search of its ground.[75] Thus, holding China to American democratic standards at this stage might be unrealistic.[76]

It is also important to note that the Communist Party, just like the People's Action Party of Singapore, has achieved the above-mentioned economic success without relaxing political control.[77] The Communist Party is likely here to stay.[78] It will continue to keep a tight grip on the economy, at times making decisions that directly affect business ventures out of purely political ambitions.[79] While economic progress and foreign investment to China drives its global dominance, political and social stability within the country is its number one priority.[80]

Likewise, "China's foreign policy behavior, including its cyber activity, is driven primarily by the domestic political imperative to protect the longevity of the Chinese Communist Party."[81] All of the objectives, such as ensuring stability, territorial integrity, innovation, and continuing economic growth, while taking steps to prepare for a possible militarized cyber conflict, support the continuation of the Communist Party.[82] Laws and regulations in China allow for flexibility of interpretation, which benefits Chinese nation's interests.[83]

Preservation of the economic activity through information and communication technology becomes any nations' primary objective when safeguarding cyberspace.[84] Cybersecurity is integral to economic prosperity,[85] which is why countries must secure activities like banking, services, administration, and so forth, to protect the stakeholders and

74. CHOW & HAN, *supra* note 18, at 20; *see, e.g*, Bauml, *supra* note 2, at 724.

75. *See* Bauml, *supra* note 2, at 725.

76. *Id.*

77. Special Report, *The Singapore Exception*, THE ECONOMIST (Jul. 18, 2015), https://www.economist.com/news/special-report/21657606-continue-flourish-its-second-half-century-south-east-asias-miracle-city-state ("Singapore is [...] the only one among the world's richest countries never to have changed its ruling party"); *see generally* CHOW & HAN, supra note 18 (noting China's economic progress over the years despite the strong hold of the Communist Party on this developing country).

78. CHOW & HAN, *supra* note 18, at 21.

79. *Id.*

80. *Id.*

81. Amy Chang, *Warring State: China's Cybersecurity Strategy*, CTR. FOR A NEW AM. SECURITY, 7 (Dec. 2014), https://s3.amazonaws.com/files.cnas.org/documents/CNAS_WarringState_Chang_report_010615.pdf.

82. *Id.*

83. *Id.*

84. PASCAL BRANGETTO & MARI KERT-SAINT AUBYN, ECONOMIC ASPECTS OF NATIONAL CYBER SECURITY STRATEGIES, PROJECT REPORT, 9 (2015), https://ccdcoe.org/sites/ default/files/multimedia/pdf/Economics%20of%20cybersecurity.pdf.

85. *See id.*

increase their societies' wealth.[86]

2. "Made in China" technology protectionism.

After the reforms of 1978, China quickly became an important player in the world trade market.[87] China's fame as the world's largest exporter of goods is familiar to anyone who has ever bought a product "made in China."[88] The influxes of foreign direct investment and access to the world's most valuable technology via multinational companies (MNC's) established in China has made China's foreign trade an engine of economic development.[89] Domestic Chinese enterprises inevitably absorb the intellectual property of companies entering the Chinese market and begin to close the technology gap, enabling China to become ever so competitive in the global marketplace.[90] Also, the undervaluation of the Renminbi allows China to keep its goods at prices, which are lower than market exchange rate, increasing its exports.[91]

The common perception in China is that the United States is constantly critiquing Chinese actions in the world market and its protection of intellectual property rights.[92]

Consequently, China is extremely sensitive to any heavy-handed tactics by foreign countries, which it usually meets with resentment.[93] This influences the isolationist view of the Chinese government, which often feels pressured by other nations into an unwanted westernization of its principles.

In recent years, the strive for technological independence has led China to increase its Internet security and to further develop its own information technology (IT). In the beginning of 2014, China pushed the development of Chinese operating systems based on Linux.[94] The

86. *Id.*

87. Reuters Staff, *TIMELINE: China Milestones Since* 1978, REUTERS (DEC. 7, 2008, 11:33 PM), https://www.reuters.com/article/us-china-reforms-chronology-sb/timeline-china-milestones-since-1978-idUKTRE4B711V20081208.

88. Investopedia, *What Country is the World's Largest Exporter of Goods?* (Jan. 19, 2015, 9:11 AM), http://www.investopedia.com/ask/answers/011915/what-country-worlds-largest-exporter-goods.asp.

89. CHOW & HAN, *supra* note 18, at 29-30 (if for example, an MNC establishes a subsidiary in China to manufacture complex machinery, the MNC has to give access to Chinese counterpart to its proprietary technology).

90. *Id.* at 319.

91. *Id.*

92. CHOW & HAN, *supra* note 18, at 325.

93. *Id.*

94. Hauke Johannes Gierow, *Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses*, CHINA MONITOR, Issue 2, (Apr. 22, 2015), https://www.merics.org/sites/default/files/2017-09/China_Monitor_22_Cybersecurity_EN.pdf.

idea was to run it on computers used in the government sphere and security relevant businesses.[95] China has been enforcing stringent limitations on the use of foreign tech, fearing network surveillance via installed back doors and the threat to its national security.[96] Sealing off the internal market from external impacts, promotes policies of industrial and innovative development and further bolsters the competitiveness of domestic companies.[97] In spite of its great progress in the technological field, China still depends on foreign high-tech.[98]

State-run telecommunications companies (China Telecom, China Unicom, and China Mobile) dominate the market with their investments.[99] Decisions they make, usually approved by the government, determine what kind of technologies will be developed, thus defining the framework for the industry and its regulation.[100] Additionally, the Chinese government endorses its own technological standards through state-run programs, generally in close collaboration with IT companies like ZTE, Lenovo, and Datang Mobile for instance.[101] However, it is not clear whether China's strive for independence will enhance network security as a whole.[102] Unfortunately, many IT companies in China still ignore crucial quality standards required for software security.[103]

The reliance of domestic companies on Chinese encryption methods poses yet another problem.[104] Unlike the international encryption standards, such as Rivest-Shamir-Adleman (RSA),[105] domestic ones allow only partial protection.[106] Chinese suppliers have to deposit a type of 'skeleton key' with the National Encryption Leading Group, which unsurprisingly gives the government in Beijing access to important data.[107]

---

95. *Id.*
96. *Id.*
97. Gierow, *supra* note 92.
98. *Id.*
99. *Id.*
100. Ernst Dieter & Naughton Barry, *China's Emerging Industrial Economy: Insight from the IT Industry*, in CHINA'S EMERGENT POL. ECON.: CAPITALISM IN THE DRAGON'S LAIR, 39, 39–59 (Christopher A. McNally ed., 2008).
101. Gierow, *supra* note 92.
102. *Id.*
103. *Id*.
104. *Id*. at 3.
105. RSA is a public-key cryptosystem, used for secure data transfer, specifically for data transmission "over an insecure network such as the Internet." Margaret Rouse, *RSA Algorithm (Rivest-Shamir-Adleman)*, TECHTARGET (last visited on Oct. 4, 2017), http://searchsecurity.techtarget.com/definition/RSA.
106. *Id*.
107. Christopher T. Cloutier & Jane Y Cohen, *Casting a Wide Net: China's Encryption*

Starting from 2015, fifteen percent of computers in official offices across China have started to convert from Windows to Chinese owned operating systems.[108] The Chinese government highly promotes NeoKylin OS and Red Flag Linux systems.[109] The problem is that Chinese technologies are not reliable yet.[110] Compared to Western-run applications, the alternative operating systems China offers[111] have a lot more security drawbacks with numerous virus-infested apps.[112]

Mandatory Internet censorship is another problem for Chinese companies, exacerbating international criticism of isolationism and protectionism.[113] The Chinese government explains that Internet restrictions, like the blocking of Google and Facebook, promote security and protect Chinese citizens against terrorism.[114] Abiding by the Chinese government's restrictions gets expensive.[115] "The existing Chinese microblogging sites have had to invest in huge armies of individuals who spend their time looking through the content and determining what should or shouldn't be removed."[116] Thus, censorship affects freedom of speech and impacts the economy of the whole country.[117]

Foreign companies unquestionably feel the impact of Chinese censorship and exposure to cyber attacks.[118] International collaboration with services such as Gmail, Google Docs, and Dropbox are increasingly

---

restrictions, WORLDECR (Nov. 2011), http://www.kslaw.com/imageserver/KSPublic/library/publication/2011articles/11-11WorldECRCloutierCohen.pdf (For a definition of RSA algorithm see Margaret Rouse, *RSA Algorythm (Rivest-Shamir-Adleman)*, TECHTARGET.COM (last visited Jan. 13, 2017), http://searchsecurity.techtarget.com/definition/RSA).

108. Gierow, *supra* note 92*,* at 4–5.

109. *Id.* at 3.

110. *Id.*

111. Gierow, *supra* note 92, at 4 (Google Play, for example, is blocked in China, so companies like Baidu, Tencent or Qihoo 360 offer substitute app stores).

112. *Id.* (citing Max Eddy, *Nearly 7,000 Malicious Android Apps Infest China's Appstores*, PCMAG.COM (Aug. 27, 2013, 2:05 PM), http://securitywatch.pcmag.com/mobile-security/315218-nearly-7-000-malicious-android-apps-infest-china-s-appstores) ("The Anzhi and EoeMarket [app] stores were the worst offenders.").

113. *Id.*

114. Reuters, *China is Another Step Closer to Controversial Cybersecurity Law*, FORTUNE (June 27, 2016, 5:22 AM) http://fortune.com/2016/06/27/china-moves-toward-adopting-cybersecurity-law/ [hereinafter *Controversial Cybersecurity Law*].

115. Victor Luckerson, *Why China is a Nightmare for American Internet Companies*, TIME (Feb. 27, 2014), http://time.com/10178/why-china-is-a-nightmare-for-american-internet-companies/.

116. *Id*. (quoting Ryan Budish, a fellow at Harvard's Berkman Center for Internet and Society).

117. *Id*.

118. *See id.* (Apple example: Lorenzo Franceschi-Bicchierai, *Apple Addresses iCloud Attacks While China Denies Hacking Allegations*, MASHABLE (Oct. 21, 2014), http://mashable.com/2014/10/21/apple-icloud-attacks-china/).

dysfunctional.[119] The same goes for virtual private networks (VPNs), restriction of which "might lead to weaker data security and trade secrets being leaked to Chinese competitors."[120] "If connections are slow or VPNs unstable," certain applications that foreign companies use for work-related purposes cannot always be accessed from China.[121] "Even simply transferring files to colleagues in other countries can be a trying experience."[122]

III. IDENTIFICATION OF THE LEGAL PROBLEM

There are two main problems in the area of cybersecurity law: 1) multiple jurisdictions, with different and conflicting laws, fracturing what should be a "globally integrated public sphere," and 2) "the risk of authoritarian or repressive regulation by nondemocratic" countries.[123]

The "piecemeal nature" of international cybersecurity regulations leaves gaping holes in cybersecurity policy and security.[124] To meet those needs one must approach a "cybersecurity regime not as geographically divided parts, but as a unified whole in a borderless cyberspace."[125] The world's super powers, like the United States and China, should set aside their differences and adopt a more centralized and mutual approach to cybersecurity. However, unfortunately, it does not seem likely to happen.

President of the United States Barack Obama when talking about "norms of state conduct in cyberspace," said that those norms do not require swapping a "customary international law" for new regulations.[126] He suggested that "[l]ong-standing international norm guiding state behavior—in times of peace and conflict—[should] also apply to cyberspace."[127] The term "international norm," however, as referenced

119. Gierow, *supra* note 92, at 5.

120. Asia-Pacific News, *China Clamping Down on Use of VPNs to Evade Great Firewall*, CNBC (Jul. 20, 2017, 3:17 AM), https://www.cnbc.com/2017/07/20/china-clamping-down-on-use-of-vpns-to-evade-great-firewall.html; *see* Arthur Charles, *China Cracks Down on VPN Use*, THE GUARDIAN (May 13, 2011, 11:41 AM), http://www.theguardian.com/technology/2011/may/13/china- cracks-down-on-vpn-use.

121. Gierow, *supra* note 92, at 5–6.

122. *Id.*

123. REBECCA MACKINNON, CONSENT OF THE NETWORKED: A CALL FOR POLITICAL INNOVATION, 36–40 (2012).

124. Bagdasarova, *supra* note 2, at 1009.

125. *Id.*

126. President of the United States of America, *International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World* 9 (2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

127. *Id.*

to cyberspace is not well defined at the moment.[128] Right now there are no set rules as to what is acceptable in cyberspace.[129]

Certain observers of the Chinese nation believe that the Communist Party learned invaluable lessons from the collapse of the Soviet Union and correspondingly changed its ways of ruling for the better.[130] However, these days' people have become less hopeful, saying that the useful reforms that helped China's successful rise have passed and "a new era of hard authoritarianism has begun."[131] Essentially, if the PRC truly wants to transition to a high-income society, it must undergo at least partial democratization.[132] This would no doubt mean democratizing China's cybersecurity strategies.

IV. ANALYSIS

On the New Year's Eve of 2015, China's official state media broadcasted Xi Jinping's annual message.[133] Mr. Xi spoke to his audience about the year to come, saying that 2016 was going to signify "the beginning of the decisive phase" of China's efforts to build a "moderately prosperous society."[134] Soon after, cybersecurity issues and enhancement of the protections against hacking and terrorism became the main focus of the decisive phase President Xi spoke of.[135]

At the same time, the new Cybersecurity Law (the Law) served as a confirmation that when it comes to the Internet, China will take an independent stance.[136] The whole host of regulations approved by the "country's rubber-stamp Parliament" in 2016, showcase the way cyberspace is managed there.[137] Ironically, comments on Chinese news and social media sites were largely censored after the state news media revealed the Law's enactment.[138]

---

128. Lee, *supra* note 51, at 960.

129. Science Monitor, *supra* note 33.

130. Chinese Politics, *A Crisis of Faith* 23, 25, THE ECONOMIST (Jan. 16, 2016), https://www.economist.com/news/briefing/21688399-their-response-wobbly-markets-chinas-leaders-reveal-their-fears-crisis-faith [hereinafter *A Crisis of Faith*].

131. *See id.* (internal quotation marks omitted).

132. *Id.*

133. *A Crisis of Faith*, *supra* note 131, at 23.

134. *Id.*

135. Adam Segal, *Chinese Cyber Diplomacy in a New Era of Uncertainty*, HOOVER WORKING GROUP ON NAT'L SECURITY, TECH. & L., Aegis Paper Series No. 1703 (June 2, 2017), https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.

136. *See* Paul Mozur, *China's Internet Controls Will Get Stricter, to Dismay of Foreign Business*, THE NEW YORK TIMES (Nov. 7, 2016), http://www.nytimes.com/2016/11/08/business/international/china-cyber-security-regulations.html.

137. *See id.*

138. *Id.*

Even before the Law was enacted, it caused an enormous uproar in the international business community.[139] The Head of Asia Securities Industry and Financial Markets Association told a forum in Hong Kong that the rules in the CSL were "worrying."[140] The expansive Law and the Anti-Terrorism Law, which took effect on January 1st, 2016.[141] The regulations indicate that the Cyberspace Administration of China (CAC) is ultimately in charge of setting the agenda of the broader set of policies concerning the CSL.[142] The bill affects both domestic and foreign companies operating in Mainland China and spans over a wide range of activity in the sphere of the Internet and information communications technologies.[143]

The Law is significant in scope and potentially overreaching in effect.[144] As China's first omnibus privacy and security regulation in the cyber realm, the CSL increases data protection in many aspects, but brings possible compliance challenges for the global community.[145] It is particularly worrisome for businesses with "significant online/digital presence," enterprises dependent on a telecommunications network, or the ones who rely on cross-border movement and sharing of business data.[146]

James Zimmerman, chairman of the American Chamber of Commerce in China described the sweeping CSL as "a step backward

---

139. Reuters, *Business Groups Slam China's Draft Cybersecurity Rules*, S. CHINA MORNING POST (Aug. 12, 2016, 12:47 AM) http://www.scmp.com/news/china/economy/article/2002550/business-groups-slam-chinas-draft-cybersecurity-rules (Letters from 46 organizations to premier Li Keqiang said that cybersecurity regulations China was drafting would constrain trade and urged to revise them).

140. Reuters, *China Cybersecurity Law Likely to Harm Foreign Firms Operating on the Mainland, Says Asia Finance Body Chief*, S. CHINA MORNING POST (Nov. 8, 2016, 4:25 PM), http://www.scmp.com/news/china/policies-politics/article/2044033/china-cybersecurity-law-likely-harm-foreign-firms.

141. Counter-Terrorism Law of the People's Republic of China (Passed by the 18th Session of the Standing Committee of the 12th National People's Congress on December 27, 2015), https://www.chinalawtranslate.com/反恐怖主义法-（2015), /?lang=en (discussing Chinas definition of terrorism, placing restrictions on the reporting of terrorist attacks and requirements for tech companies to provide support for counter-terrorism purposes); *see also* Zunyou Zhou, *Chinas Comprehensive Counter-Terrorism Law* (Jan. 23, 2016), https://thediplomat.com/2016/01/chinas-comprehensive-counter-terroJan. 23, 2016rism.

142. Mozur, *supra* note 137.

143. *China Adopts a Tough Law*, *supra* note 142.

144. Baker & Mckenzie, *Final Passage of China's Cybersecurity Law* (Nov. 25, 2016), http://www.bakermckenzie.com/en/insight/publications/2016/11/final-passage-of-chinas-cybersecurity-law/.

145. Gabriela Kennedy & Xiaoyan Zhang, *China Passes Cybersecurity Law* (Nov. 18, 2016), https://hk-lexiscn-com.libproxy.scu.edu/topic/legal.php?tps=cp&act=detail&id=204423&newstype=3&isEnglish=Y.

146. Baker & McKenzie, *supra* note 158.

for innovation in China that won't do much to improve security."[147] According to Chinese officials, the CSL is primarily designed to strengthen local networks against malicious hacking.[148] However, in the eyes of foreign businesses, this piece of legislation looks very much like "a techno-nationalist Trojan horse."[149]

As a first comprehensive Law on cybersecurity, the CSL's provisions are still very general and vague.[150] A lot will depend on the implementing regulations and standards to be issued by the State Council, the CAC, Ministry of Public Security,[151] and the Ministry of Industry and Information Technology.[152]

Some of the Law's content repeats existing rules adopted by China over the years and simply combines separate regulations into one.[153] Prior existing rules were scattered under different regulations.[154] The PRC believes that forming one unified Law improves enforcement and notifies the business community, as well as the general public, of the unprecedented cybersecurity threats within and beyond China's borders.[155] However, the power given to Chinese authorities under the CSL seems to have no limit.[156]

1. Protection of key information infrastructure.

Article 31 of the CSL says in part:

> The State shall . . . focus on protecting both the key information infrastructure used for public communications and information service, energy, transport, water conservancy, finance, public services, e-government affairs and other important industries and fields and other key information infrastructure that will result in serious damage to the national security, national economy and people's livelihood and public interests if they are destroyed, there are lost functions or they are subject to data leakage. The State

147. *China Adopts a Tough Law*, *supra* note 142.
148. *Id.*
149. *Id.*
150. Dr. Ulrike Glueck & Sammie Hu, *PRC Cyber Security Law—What are the Most Important Impacts on Foreign Businesses?*, LEXICOLOGY (Jul. 3, 2017), https://www.lexology.com/library/detail.aspx?g=87d2de53-1499-46f9-8a1d-d5a8886c4d15.
151. Dong, *supra* note 152, at 2.
152. Baker & McKenzie, *supra* note 158.
153. Samuel Yang, *The New China Cybersecurity Law—Why Companies Should Care But Not Panic?*, ANJIE LAW FIRM (Nov. 14, 2016), https://hk-lexiscn-com.libproxy.scu.edu/topic/legal.php?tps=cp&act=detail&id=203916&newstype=3&isEnglish=Y.
154. *Id.*
155. *Id.*
156. Kennedy & Zhang, *supra* note 159.

> encourages network operators other than key information infrastructure to participate in the protective system of key information infrastructure on a voluntary basis.[157]

The CSL introduced the concept of key information infrastructure (KII) for the first time and imposed a series of heightened obligations for operators of KII.[158] The definition of "key" or "critical," as certain sources call it, is broader than anyone expected.[159] Although not every company's information technology infrastructure will likely be regarded as a KII, as it appears to be limited to those involving "national security, national economy and the people's livelihood, or the public interest."[160] This definition is nevertheless overly broad and the State Council will have to define a more narrow scope of the KII later.[161] The State Council will also likely have to specify the mandatory security measures that organizations operating KII will need to apply.[162] The government has considerable leeway to bring industries not specifically singled out in the definition into the scope of the legislation at a later stage.[163] Such leeway helps the Communist Party to stay in control.[164]

2. Information and data storage requirements for business entities.

Article 37 of the CSL says:

> *Key information infrastructure* operators shall store personal information and important data gathered and produced during operations within the territory of the People's Republic of China. Where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in concert with the relevant departments under the State Council. Where the laws and administration regulations have other provisions, those provisions

157. The Law, *supra* note 151.

158. Dong, *supra* 152, at 3 (this source uses the term critical information infrastructure, however, different sources use terms "key" and "critical" interchangeably).

159. *China Adopts a Tough Law*, *supra* note 142.

160. Yang, *supra* note 167.

161. Final Cybersecurity Law Enacted in China, Privacy & Information Security Law Blog (Nov. 8, 2016), https://www.huntonprivacyblog.com/2016/11/08/final-cybersecurity-law-enacted-china/ [hereinafter Privacy & Information].

162. *Id.*

163. Kennedy & Zhang, *supra* note 159.

164. *See* National Security, *Everything Xi Wants*, THE ECONOMIST (Jul. 4, 2015), https://www.economist.com/news/china/21656689-new-national-security-law-hints-communist-partys-fears-everything-xi-wants.

shall prevail.[165]

The general interpretation of this provision points to the obligation for foreign companies to keep servers for users in China within China's borders.[166] Even with an increase in cost, many foreign companies have already complied with this requirement.[167]

The overly broad residency requirements place entry obstacles for both Chinese and foreign entities, which can hinder economic growth.[168] This storage provision separates China from the global digital economy.[169] Positions like this bring China closer to cyber sovereignty that it desires, but also make companies distrust the safekeeping of their data while on Chinese territory. Those companies worry that the Law will require additional expenses and increase the risk of data theft.[170]

The security assessment provision creates yet another barrier for businesses who want to break into China's market.[171] Chinese KIIs, under the literal reading of the CSL, must undergo a stringent assessment by relevant Chinese authorities prior to any cross-border information transfer.[172] The security assessment requires business entities to identify the need for data export and creates the risk of personal information being leaked along with potential compromises to national security.[173] Article 38 specifies the requirement for operators of KII to undergo a network security assessment at least once a year and "submit the detection and assessment situations as well as improvement measures to the relevant departments."[174] The Secretariat of the National Information Security Standardization Technical Committee has issued a "Draft for Comment" with an October 2017 deadline for concerned entities to submit opinions on the security assessment of cross-border information transfer.[175] So presently, the Chinese authorities still have

165. The Law, *supra* 151 (emphasis added).

166. Josh Horwitz, *China's Bewildering New Cybersecurity Law is Keeping Foreign Tech Firms Out of the Country*, QUARTZ (Nov. 7, 2016), http://qz.com/829248/chinas-new-cybersecurity-law-is-so-vague-that-its-keeping-foreign-tech-firms-out-of-the-country/ (For instance AirBnB, over a year after it entered the Chinese market via a joint venture, announced that it would move its Chinese user data to a Chinese location).

167. *Id.*

168. *Controversial Cybersecurity Law*, *supra* note 112.

169. *Id.*

170. *China Adopts a Tough Law*, *supra* note 142.

171. *See* Kennedy, *supra* note 155.

172. *Id.*

173. *China's Cyber Security Law: With More Questions than Answers*, *What Steps Can You Take Now?*, MORRISON & FOERSTER (Jul. 31, 2017), https://www.mofo.com/resources/publications/170731-chinas-cyber-security-law.html.

174. The Law, *supra* note 151.

175. *Comments Sought on the Information Security Technology—Guidelines for Security Assessment of Data Cross-border Transfer and Other Five National Standards*,

to decide on how, when, and at what cost the security assessments will take place.

The residency, data storage and security assessment provisions make it challenging for businesses to operate in China. Underscoring the possible glooming outcome for many international companies in China, Baker & McKenzie specialists point out that: "[i]n a worst-case scenario, many foreign business operators may be required to carve-out China from their global or regional technology, infrastructure/backbone, and/or become mired in time-consuming regulatory approvals for the export or sharing of data with entities outside China."[176]

3. A new provision on the protection of network security.

"Networks," according to Article 76 of the CSL, includes networks and systems that are composed of computers and other information terminals or facilities used to "collect, save, transmit, exchange, and process information."[177] Network operators mandatorily follow all the legal obligations under the CSL.[178] The Law also maintains that promoting and "safeguarding the national cyberspace sovereignty" within the networks is a fundamental principle.[179]

The list of further obligations (and sadly no rights) for network operators under Articles 21, 24, 25, and 28 respectively include: the compliance with the requirements of tiered system for cybersecurity protections; the authentication of users' real identity; the formulation of cybersecurity emergency strategies; the assistance and support for investigative authorities.[180]

The panic caused by all the obligations that the companies have to abide by, may be unsubstantiated.[181] The new Law brings back the concept of the "tiered system" of cybersecurity protections, familiar to businesses, which have complied with 1994 Regulations for Safety

---

https://hk.lexiscn.com/latest_message.php?id=241041&isSearchResult=1&url=news.php%253Fact%253Ddetail%2526id%253D241041&access=content_detail&lang=cn ("[t]he Draft for Comment sets forth procedures, key points and methods for the security assessment of the cross-border transfer of personal information and important data") (citing to关于征求《信息技术 安全技术 匿名实体鉴别 第4部分：基于弱秘密的机制》等6项国家标准意见的通 , National Information Security Standardization Technocal Committee (Aug. 30, 2017, http://www.tc260.org.cn/zdetail_g.jsp?id=20170830193813).

176. Baker & McKenzie, *supra* note 158.

177. Dong, *supra* note 152, at 2.

178. *Id.*

179. *Id.*

180. *Id.*

181. *See* Yang, *supra* note 167 (The Administrative Measures for Hierarchical Protection of Information Security in 2007 also classified information into tiers with higher ones concerning national security issues).

Protection of Computer Information Systems.[182] Rules regarding network access, domain registration, fixed or mobile phone, information publication and instant messaging services, which require users to provide their real identity information, are restatements of the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection (2012).[183] The fact that the Law incorporates multiple restatements of the older regulations signifies that businesses, with established presence in China, may have compliance polices already in place and should not worry about the new Law's requirements.[184]

However, grounds for worrying still exist. The provision requiring certification for important network equipment and software, for instance seems deceitful.[185] As foreign companies, aware of China's pirating history, fear that compliance will require turning over security keys and core tech, which could be "shared with" state-owned competitors.[186] Similarly, Article 10's provision, requiring the construction and operation of Internet services that are secure and stable, are likely to advantage Chinese hardware firms like Lenovo and Huawei and local cloud operating providers like Tencent or Alibaba.[187]

Article 65 provides that KII operators might violate the Law if their products or services have not passed safety inspections.[188] A threat of such violations of the Law is especially worrisome because the nature of the safety inspections remains unclear.[189] In a similar fashion, Article 21 states that "specialized network security products" must meet a set of standards released in a "catalog" by the State Council, which are yet to be revealed.[190]

4. Government supervision, security reviews, and technical support

The security reviews for information and communications technology products and services under new rules constitute technical barriers to trade under the World Trade Organization and may potentially undermine the security of data.[191]

According to the CSL, network operators must provide technical

182. *Id.*
183. *Id.*
184. *Id.*
185. *China Adopts a Tough Law*, *supra* note 142.
186. *Id.*
187. *Id.*
188. Horwitz, *supra* note 180.
189. *Id.*
190. *Id.*
191. *E.g.*, *Controversial Cybersecurity Law*, *supra* note 112.

support and assistance to public or national security agencies when investigating a crime.[192] Additionally, network operators are required to adopt technical measures to oversee and record their operations and to preserve related logs for at least 6 months.[193]

Also, under Article 22, network and service providers have to inform the users and relevant authorities if any security or bug has been detected.[194] This requirement obligates providers to offer constant security maintenance and prohibits them from installing malware in their products.[195] Article 23 requires key network facilities to comply with relevant national standards and compulsory certification requirements.[196] For example, such facilities can only be offered for sale once they have complied with the certification provision from the qualified organization.[197] All the unnecessary burdens for network operators and service providers contribute to the overall apprehension of the China's market participants.

5. Protection of Personal Information.

Regarding the protection of personal information, the CSL restates the obligations, which have already existed across the PRC's laws and regulations.[198]

The familiar privacy laws' requirements restated in the new Cybersecurity Law include informed consent and the use of personal information only for a purpose agreed upon by the relevant individual.[199] Provisions on the collection and use of the personal information also reiterate the "principles of legitimacy, rightfulness and necessity."[200] Article 42 requires the adoption of security protection measures for personal information and incorporates new provisions like data breach notification requirements and data depersonalization as an exception to

192. Privacy & Information, *supra* note 175 ("If it is ultimately unwilling to offer reciprocal access to its own market, China cannot assume that it will indefinitely continue to enjoy open and unhindered access to the [other]'s," the EU Chamber president Joerg Wuttke said).

193. *Id.*

194. Dong, *supra* note 152, at 2–3.

195. *Id.* at 3.

196. *Id.*

197. *Id.*

198. Dong, *supra* note 152, at 3 (*See* the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection (2012), the Provisions on the Protection of Personal Information of Users of Telecommunications and Internet Services (2013) and the Law on the Protection of Consumer Rights and Interests (2013 Revision)).

199. Privacy & Information, *supra* note 175.

200. *Id.*; *See* Article 41, Law, note 151 (quoting the Article).

inform and consent requirements.[201] The consent exception for data that cannot identify specific individuals "is believed to be a major win for companies engaging in Big Data business such as online precision marketing companies using cookies technologies."[202] The breach notification requirements, introduced for the first time, might magnify the adverse effects to the public image of the data controllers and processors.[203] Therefore, companies should consider this when developing crisis management strategies.[204]

Article 43 adds an individual right to question the correctness or request deletion of personal information in cases where the information is inaccurate or used for a purpose not agreed upon.[205] Additionally, theft and illegal sale of personal data have already been criminalized in China under Amendment No. 7 (2009) and Amendment No. 9 (2015) to the PRC Criminal Law.[206] These penalties for breach are considerably harsher than the ones before:

> Breach of the new law will be subject to, according to the seriousness of the breach, penalties such as warning, order of correction, fines (up to RMB 1,000,000), forfeiture of illegal gains, suspension of business, and/or revocation of operation permit and business license. Individual wrongdoers are also subject to a fine of up to RMB 1,000,000, detention, fixed-term or lifetime ban for key positions in the network security and network operation areas, and/or even criminal penalties.[207]

B. The CSL's vague language

China critics say the country uses extremely vague wording in its legislations to give flexibility to policymakers on how to implement laws.[208] Keeping the laws so vague that they are impossible to follow, has essentially been a "tried-and-true tactic" employed by the PRC to keep foreign companies away from China.[209] The unfortunate lack of clarity on how to comply with the Law is a huge turn off for overseas enterprises.[210] "Foreign companies who have the technology and have the impetus to get into the China [are] not getting the necessary

201. Dong, *supra* note 152, at 3.
202. Yang, *supra* note 167.
203. *Id.*
204. *Id.*
205. Dong, *supra* note 152, at 3.
206. Yang, *supra* note 167.
207. *Id.*
208. *Id.*
209. Horwitz, *supra* note 180.
210. *Id.*

information to do so. And since the information isn't there, they're shut out of the market."[211]

The CSL puts businesses in danger of government meddling or losing business in the world's second largest economy. Uncertain, vague language of the Law creates an uncertain business environment. Foreign companies willing to see how this Law untangles will no doubt have a chance to succeed, but the risk is real and the penalties for non-compliance are harsh. After June 2017, the foreign investors tempted into entering the Chinese market are bound to face challenges directly related to the new Law.

On the positive side, the regulations might not significantly change the ordinary course of business.[212] Many of the rules have already been in effect, just not codified. Samuel Yang Honqquan, a partner of AnJie Law Firm suggests that:

> [I]nstead of trying to seek the hidden meanings of the new law and overstating its downsides, [foreign companies doing business in China] should watch closely the policy changes in their own industries where special rules may be issued by the regulators having a more direct impact on the ways of doing business of these foreign companies.[213]

V. PROPOSAL

Cybersecurity has become a significant area of international and domestic concern.[214] To address this issue the United States and China have released various cybersecurity strategies.[215] Unfortunately, those strategies did not gain much momentum. These two superpowers need a more viable strategy that will actually stick.

Security surveillance and cyber confrontations that the United States and China engage in, hurt both countries' economies and undermines the protections of their IP networks. China's vague laws and overreaching security requirements restrict freedom of speech and throw

---

211. *Id.*

212. Mozur, *supra* note 137.

213. Yang, *supra* note 167.

214. *See* Joint Communication to the European Parliament, the Council of European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, at 3, COM (2013) 1 final (July 2, 2013).

215. *See* Exec. Office of the President, International Strategy for Cyberspace: Prosperity Security, and Openness in a Networked World 2 (2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; China addressed same concerns in its draft resolution - "International Code of Conduct for Information Security," in partnership with Russia and other countries.

up barriers to global companies. In the United States, cyberspace is talked about like it is the ocean, where nobody owns it and people can just traverse through it as they please.[216] U.S. companies like AT&T or Verizon, actually own quite a bit of it.[217] And even though federal government cannot always compel everyone to act,[218] the cyber-law literature suggests that cyberspace can be effectively regulated considering that physical facilities that make the online activity possible are subject to government control.[219] Additionally, companies have to themselves strive to improve the infrastructure within the private sector.[220]

The cyber community points out that certain national government actions may negatively affect another nation or its citizens.[221] "As one national government doesn't have sovereignty over another, the latter's behavior will not be subject to former's regulations."[222] This presents a great flaw in the international law, and limits what a nation like the United States can do in response to another nation's, such as China's, aggressive attack, or vice versa.[223]

Luckily, the PRC is not completely averse to international cooperation on cybersecurity.[224] Even though unsurprisingly, China's and other countries' "International Code of Conduct for Information Security" proposal defended the legitimacy of the governments' control of the online flow of information, read positively, it did try setting at least some rules for proper cybersecurity behavior.[225]

Because both countries' privacy and cybersecurity systems are flawed, but not hopelessly so, I propose the European Union approach to cybersecurity which rejects an idea of governmental scrutiny and a contention that civil societies cannot have free will when it comes to the use of technology.[226]

---

216. Science Monitor, *supra* note 33.

217. *Id.*

218. *Id.*

219. Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* at 49–63 (Oxford University Press, Inc., 2006).

220. *Id.*

221. Lee, *supra* note 51, at 959.

222. *Id.*

223. *Id.*

224. *Id.* at 962 (In September 2011 China, Russia, Tajikistan, and Uzbekistan, drafted a resolution titled "International Code of Conduct for Information Security," and presented it to the United Nations General Assembly. International Code of Conduct for Information Security, U.N. Doc. A/66/359 (Sept. 14, 2011).

225. *Id.* at 962–63.

226. *See generally* Darmois & Schmeder, *supra* note 12 (discussing that constant government oversight is damaging to free societies).

Cyberattacks have increased in scope and quantity in recent years. They undermine not only national security of the countries around the world, but also the free flow of information and free trade. Thus, an international cybersecurity treaty is in order. However, such a treaty would only be successful if the principal actors of the global community would craft something mutually beneficial and make an earnest effort to comply with it, leading by example. Super powers feel like they have to support a defensive and offensive approach in their military and economic cyber policies, but when it comes to civil societies, governments are not as compelled to defend them.[227] The EU stands for an approach that gives the civil societies a sense of security they need when it comes to cyber threats.[228] Unlike the United States and China, that approach the issue of security in cyberspace through the logic of national security and cyber superiority, the EU approach is legalistic and protective.[229] The EU cybersecurity concept focuses on fighting cybercrime, and on resilience to ensure rapid recovery from cyber attacks.[230] EU capability development focuses on building capacities that enable detection, response, and recovery from sophisticated cyber threats.[231] In the military field, the EU is engaged in cyber self-protection and assured access to cyber space to enable its operations and missions.[232]

At this point, the EU can help build consensus on cyber-security issues in the international community. Also, if both the United States and China would support a European framework regarding cybersecurity, the EU would be more open to establishing definite international norms that would prevent the threat of covert offenses by various states.

CONCLUSION

It is incredibly difficult to justify a Law which places censors on the freedom of expression, is costly for trade and innovation, and creates friction between the global powers. Terrorism, whether in the physical world or cyber realm, does not exist because of Google or Facebook, as China implicates. Social media, which does not promote an immoral society or uncivilized behavior, could even work to China's favor in

227. *Id.* at 9–10.
228. *See id.*
229. *Id.* at 17.
230. *Id.*
231. *Id.*
232. Darmois & Schmeder, *supra* note 12, at 15.

advancement "of the core socialist values."[233] In addition, other ways exist to address the growing threats of cyberattacks domestically and on the global arena. China's sweeping new Cybersecurity Law is not one of those ways.

Chinese officials should listen to Eric Xu,[234] who more than a year ago warned: "If we're not open, if we don't bring in the world's best technology, we'll never have true information security."[235] That eloquent rejection of techno-nationalism came from a man who is co-chief executive of Huawei.[236]

The United States is likewise not cyber efficient at the moment. The country often engages in political espionage and hacking with the goal of preventing terrorist attacks, yet at the same time, it critiques similar actions coming from the Chinese government. At some point the United States has to become more concerned about public use of protective technologies and less involved in the behavior that perpetuates the conflict between the two countries.

Since neither country's cybersecurity strategies have worked much to their advantage, both the United States and China need to consider taking a different route. The EU approach can not only be beneficial to both superpowers, but also unify the rest of the international community on issues surrounding cybersecurity. Cybersecurity is inherently transnational. Thus, China cannot isolate itself from the rest of the world, as the country wants to do. For the United States, a new strategy would give an opportunity to improve and focus on the protective means of cybersecurity, which in turn will help fight the cybercrimes and prevent the unwanted cyberattacks.

233. Bochen Han, *How Much Should We Read into China's New "Core Socialist Values"?*, COUNCIL ON FOREIGN RELATIONS (Jul. 6, 2016), https://www.cfr.org/blog/how-much-should-we-read-chinas-new-core-socialist-values.

234. *China adopts a tough law*, *supra* note 137.

235. *Id.*

236. *Id.* Huawei is a Chinese multinational networking and telecommunications equipment and services company.