Science and Technology Law Review

Volume 20 | Number 2 Article 18

June 2018

A Peek Over the Great Firewall: A Breakdown of China's New Cybersecurity Law

Jacob Quinn
Southern Methodist University

A Peek Over the Great Firewall: A Breakdown of China's New Cybersecurity Law

*Jacob Quinn**

I. INTRODUCTION

While most are familiar with the "Great Firewall of China," the Chinese government's Internet censorship against foreign websites and unfavorable speech,[1] people are less familiar with what part this firewall plays in the intricacies of China's cybersecurity regime. President Xi Jinping emphasized on multiple occasions that the Internet poses new challenges for China's interests and that the government is rightly empowered to dictate the measures securing those interests.[2] On November 7, 2016, the government promulgated a new set of cybersecurity measures against the protest of numerous foreign businesses.[3] These measures are aimed primarily at network providers who provide services the government determines crucial to the operation of services on the Internet, also known as "critical information infrastructure."[4] The law will require the providers to submit to an invasive security review and store any data collected from the users in China within the geographic boundaries of China.[5] This policy enables China's regulatory agencies to exercise wide discretion in determining which providers fall into what category, and what precise measures need to be taken to satisfy the legislation.[6] While China is not alone in creating such a state-controlled cybersecurity regime, the broad authority it gives to itself is notable, leaving little for non-government entities to do but obey.[7]

---

* J.D. Candidate, 2018, SMU Dedman School of Law; B.A. History, *cum laude*, 2015, University of North Texas.

1. Gary Brown & Christopher D. Yung, *Evaluating the US-China Cybersecurity Agreement, Part 2: China's Take on Cyberspace and Cybersecurity*, DIPLOMAT (Jan. 1, 2017), http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity/.

2. Chris Mirasola, *Understanding China's Cybersecurity Law*, LAWFARE (Nov. 8, 2016, 11:53 AM), https://www.lawfareblog.com/understanding-chinas-cybersecurity-law.

3. *Id.*

4. *Id.*

5. *Id.*

6. Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法) (promulgated by Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), art. 31, *translated in 2016 Cybersecurity Law*, CHINA LAW TRANSLATE (Nov. 7, 2016), http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en, art. 31 (unofficial translation) [hereinafter *Cybersecurity Law*].

7. Brown & Yung, *supra* note 1.

This comment discusses the foreseeable consequences of such a broad, state-controlled regime and compares such cybersecurity control to other countries' cyberspace policies. Part II lays out the general dangers in cyberspace that have given rise to systemized cybersecurity, along with the concepts in cybersecurity regimes. Part III compares China's previous efforts to establish its own cybersecurity regime to the recently passed 2016 Cybersecurity Law. Part IV compares China's presently promulgated cybersecurity regimes with those established by other prominent countries. Finally, Part V analyzes the foreseeable impact of the 2016 Cybersecurity Law, including the potential harm the law could inflict on the Chinese public, the cooling effect it could have on foreign business in China, and the consequences it could have against globalization.

II. THE LANDSCAPE OF CYBERSPACE

As the Internet becomes more of an instrumental part of our daily lives, the level of harm it could do to our society should it be misused increases.[8] Countries around the world have experienced the problems that come with wiring essential aspects of life and governance to the world wide web, exposing crucial systems to attack from half way around the world.[9] While the days of physical bombings and theft are not yet behind us, it is becoming clear that enemies of the state can wreak more havoc from cyberspace than they can with attacks in the real world.[10]

A. The Perils of the Digital Age

Threats from cyberspace come in numerous forms, but can be loosely categorized by the target of the threat and what kind of harm is intended by the attack. When an individual (a private citizen with limited connection to a business or government)[11] is targeted, the intended harm is usually theft of finances.[12] The attacker, through either an active attempt to fool the individual into giving up their personal information (e.g., bank account information,

8. *See generally* Nilesh Christopher, *The Worst Cyberattacks of 2016*, Economic Times (Dec. 28, 2016, 8:59 AM), http://economictimes.indiatimes.com/small-biz/security-tech/security/the-worst-cyber-attacks-of-2016/articleshow/56212448.cms (discussing the effect of cyberattacks causing financial information and voter data leaks, mass Internet outage, and interference in the U.S. election).

9. *See generally id.* (referring to cyberattacks in India, Bangladesh, Philippines, and the United States).

10. *See* Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance*, 62 Am. U.L. Rev. 1273, 1296–302 (2013) (outlining categories of "cyberthreats").

11. *What Is Individual?*, Law Dictionary, http://thelawdictionary.org/individual/ (last visited Feb. 2, 2018).

12. *See Internet Users Lose Rs 32,400 on an Average to Cyber Attacks*, Economic Times (Jan. 28, 2017, 5:30 PM), http://economictimes.indiatimes.com/maga

social security number, or passwords to financially sensitive accounts), or passively infecting his computer with a virus or worm, solicits enough information to commit identity theft.[13] Once the attacker is able to convince a system that he is the targeted individual, he can do anything from opening new lines of credit in the person's name, to using the person's computer as a part of a network of infected computers to attack more complex systems in a manner described below.[14] The intended harm could also be more explicitly malicious if the attack has a specific desire to harm the targeted individual.[15] Using the same methods as the attacker above, the malicious actor can expose information on the person's computer to the public, bringing all sorts of humiliating details to light.[16]

When targeting a business, the intended harm will usually be some sort of theft.[17] This theft can range from intellectual property,[18] to consumer information,[19] and private communications.[20] Such information can be used for the attacker's explicit benefits, or simply to harm the target.[21] Examples of such attacks include a theft of trade secrets from ThyssenKrupp,[22] theft of

zines/panache/Internet-users-lose-rs-32400-on-an-average-to-cyber-attacks/articleshow/56832600.cms.

13. Aashika Jaan, *How Safe Are You From Cyber Attacks?*, Economic Times (Jun. 22, 2016, 10:30 AM), http://economictimes.indiatimes.com/small-biz/security-tech/security/how-safe-are-you-from-cyber-attacks/articleshow/52851255.cms.

14. *Id.*

15. *Id.*

16. *Id.*

17. *See* Neha Alawadhi, *Cyber Attacks Cost Companies 20 Per Cent Revenues in 2016*, Economic Times (Feb. 7, 2017, 11:58 AM), http://economictimes.indiatimes.com/industry/tech/Internet/cyber-attacks-cost-companies-20-per-cent-revenues-in-2016/articleshow/57014638.cms.

18. Eric Auchard & Tom Käckenhoff, *ThyssenKrupp Trade Secrets Stolen in 'Massive' Cyber Attack This Year*, Reuters (Dec. 8, 2016, 3:45 AM), https://www.reuters.com/article/us-thyssenkrupp-cyber/thyssenkrupp-secrets-stolen-in-massive-cyber-attack-idUSKBN13X0VW.

19. *See* Pratik Bhakta, *E-Wallet Companies Grow Fast, but Not Covered for Cyber Attack*, Economic Times (Jan. 3, 2017 10:14 AM), http://economictimes.indiatimes.com/markets/stocks/news/e-wallet-companies-grow-fast-but-not-covered-for-cyber-attack/articleshow/56305712.cms.

20. Julia Boorstin, *The Sony Hack: One Year Later*, CNBC (Nov. 25, 2015, 4:42 PM), http://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html.

21. *Id.*

22. *See* Auchard & Käckenhoff, *supra* note 18.

account holders' information from financial institutions,[23] and the infamous hack on Sony.[24]

In some instances, if the business is providing a service, disruption of that service may also be the intended harm, for various reasons.[25] These disruptions are usually the result of overloading the server that handles routing information to various websites with requests (using computers that have been infected by malicious software) to the point where it freezes up.[26] A recent example of this kind of cyberattack on businesses was a paralyzing of Dyn servers, which led to the temporary shutdown of popular websites like Facebook and Twitter.[27]

When targeting a government, or an agent of the state, the intended harm will usually be theft of information,[28] dissemination of false information,[29] or a disruption of services.[30] The attacker could be anyone from a private individual with a grievance against the state,[31] an organized group trying to accomplish an agenda,[32] or another government.[33] The most obvious example of this is the National Security Agency's surveillance scheme, which exploited flaws in cybersecurity systems and data protection to monitor both foreign and domestic activities.[34] Utility services have also been subject to cyber attacks, potentially denying electricity to large segments of the

23. *See* Bhakta, *supra* note 19.

24. *See* Boorstin, *supra* note 20.

25. Nicky Woolf, *DDoS Attack That Disrupted Internet Was Largest of Its Kind, Experts Say*, GUARDIAN (Oct. 26, 2016, 4:42 PM), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

26. *Id.*

27. *Id.*

28. Matthew Funk, *Tragedy of the Commons: Snowden's Reformation and the Balkanization of the Internet*, 31 SYRACUSE J. SCI. & TECH. L. REV. 39, 49 (2015) (discussing both the NSA scandal and the impact it had on the cybersecurity policies of several countries).

29. Melissa Eddy, *After a Cyberattack, Germany Fears Election Disruption*, N.Y. TIMES (Dec. 8, 2016), https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html (discussing cyberattack on German Parliament's computer network and evidence of attempts to influence the federal election).

30. Pavel Polityuk et al., *Ukraine's Power Outage Was a Cyber Attack: Ukrenergo*, REUTERS (Jan. 18, 2017, 6:22 AM), http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA.

31. *See* Funk, *supra* note 28, at 49.

32. *See* Christopher, *supra* note 8.

33. *See* Eddy, *supra* note 29.

34. Funk, *supra* note 28, at 49–52.

population.[35] If such an attack was carried out by a foreign attacker, especially if combined with military action, the effect would be devastating.

The greatest risks a government faces are disruptions of its critical infrastructure (CI). CI is generally defined as areas that, should they suffer an attack, could cause a destabilizing effect on the country.[36] But, this definition is not universal, and what one country legally defines as falling under its CI may be something another country leaves as general infrastructure.[37] For example, the attack on Dyn, a private business, could be an attack on CI if the U.S. government considered that the connections to the various websites that Dyn supported would have a destabilizing effect if severed.[38] Other areas that are universally considered CI are public utilities (power and water management) and systems of transportation.[39]

With these threats arrayed against a nation and its citizens, it is recognized that the state should take steps to ensure its citizens, its private sector, and itself are secure from harm.[40] But, what steps should a state take? Should it interfere with private businesses (i.e., businesses not owned by the state) to ensure that the information they collect from citizens is secured? Should it prevent access to parts of the Internet, to keep citizens from straying into areas where their data can't be protected? In addressing questions like these, certain schools of thought have developed to guide the creation of many countries' cybersecurity regimes.[41]

---

35. *See* Polityuk et al., *supra* note 30.

36. *See* Exec. Order No. 13,636, 78 Fed. Reg. 11,739 § 2 (Feb. 12, 2013).

37. *See* Symposium, *Beyond The New "Digital Divide": Analyzing The Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 144 (2014) [hereinafter *Digital Divide*].

38. *See* Woolf, *supra* note 25; *see generally* Eugenia Georgiades et al., *Crisis on Impact: Responding to Cyber Attacks on Critical Information Infrastructures*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 31 (2013) (discussing various aspects of cyberattacks on industries generally considered to be CI and how the affected governments responded).

39. *See Digital Divide*, *supra* note 37, at 149 (citing William J. Lynn III, Deputy Sec'y of Def., Remarks on the Department of Defense Cyber Strategy, (July 14, 2011), http://www.defense.gov/speeches/speech.aspx?speechid=1593); *see also id.* at 153 (citing *Commission Proposal for a Council Decision on a Critical Infrastructure Warning Information Network*, at 10, COM (2008) 676 final (Oct. 27, 2008)).

40. *Id.* at 122.

41. Scott J. Shackelford & Andraz Kastelic, *Toward a State-Centric Cyber Peace?: Analyzing The Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 895, 898–99 (2015).

B. Guiding Concepts in Cybersecurity

There are two schools of thought that have arisen to help conceptualize how countries protect themselves and their citizens online.[42] These schools of thought can be seen as opposing ends of a spectrum, while presenting a false choice and denying the existence of a middle road.[43] Both schools of thought could also be seen as pipe dreams that rely on analogizing the Internet as something that it is not.[44] But, while these philosophies appear unhelpful in actually developing a workable cybersecurity regime, they can serve as guideposts for analyzing the differences between different regimes. If viewed as the extremes on a spectrum, spanning the degree of direct government control the regime asserts, these two schools of thought serve to distinguish the philosophy a government may hold when approaching how to secure cyberspace.

One extreme is recognized as "Cyber Paternalism," described elsewhere as "Data Nationalism," or "Internet Sovereignty."[45] It is the idea that physical borders cross over into cyberspace, where ports are erected to manage the flow of data into and out of a country's data storage facilities.[46] Under this concept, jurisdiction over data is exercised over the physical media.[47] To better exercise maximum jurisdiction, all the data collected within the country will be required to be stored within the country's physical borders, a process called data localization.[48] On the other hand, this concept has also been used to claim jurisdiction over a majority of the Internet, regardless of where the data is stored, by basing jurisdiction upon the concept that citizens bring a certain domain into your jurisdiction when they access it.[49]

Meanwhile, the other extreme would prefer treating the Internet like a "Cyber Commons," an open space separate from physical borders, where jurisdiction is defined more by who is managing a certain website's domain

42. Shackelford, *Toward Cyberpeace*, *supra* note 10, at 1273, 1281–82.

43. *Id.*

44. *Id.* at 1318 (stating the choice between Internet sovereignty and Internet freedom may not be necessary, as cyberspace could be treated as a "pseudocommons" in which public and private regulators cooperate).

45. *Id.* at 1303.

46. *See* Anupa Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 680 (2015).

47. *See id.* at 680.

48. *Id.* at 680–81.

49. Symposium, *Law and Borders-The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1394 (1996) ("This would be the modern equivalent of a local lord in medieval times either trying to prevent the silk trade from passing through his boundaries . . . or purporting to assert jurisdiction over the entire known world.").

than by where the data may be tangibly stored.[50] Security for the domains would be based on what could be called an industry standard, a level of care that could be used as a legal standard of care to measure companies against each other in the event of a breach.[51] This standard of care would be the result of a collaboration between the public and private sectors, businesses, consulting legislators, and experts on the best approach to enhancing cybersecurity cooperatively.[52] This is referred to as a "multi-stakeholder approach," as each of these parties are believed to have a stake in Internet governance.[53]

III. CHINA'S RESPONSE

A. Before the 2016 Cybersecurity Law

The current treatment of cybersecurity in China is best encapsulated by a statement from President Xi Jinping in early 2014: "No national security without cyber security."[54] This quote sets the tone for the protectionist measures toward "Cyber Paternalism" that are pervasive in China's cybersecurity regime, even before the passing of the 2016 Cybersecurity Law.[55] The measures include the strict regulation of software produced by western manufacturers and an attempt to foster local innovation in that same area.[56] Other objectives of the Chinese government include: increasing security, domestic production, domestic demand, and maintaining the ruling party's political power.[57]

50. *Id.* at 1378–80.

51. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 311 (2015).

52. Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 346 (2015).

53. *Id.*

54. Hawke Johannes Gierow, *Cyber Security in China: New Political Leadership Focuses on Boosting National Security*, MERCATOR INST. FOR CHINA STUDIES: CHINA MONITOR 2 (Dec. 9, 2014), http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf.

55. *Id.*

56. *See id.* at 2; *see also Digital Divide*, *supra* note 37, at 162–63.

57. *See Digital Divide*, *supra* note 37, at 162–63; *see also* Amy Chang, *Warring State: China's Cybersecurity Strategy*, CTR. FOR A NEW AMERICAN STRATEGY 12 (Dec. 2014), https://s3.amazonaws.com/files.cnas.org/documents/CNAS_WarringState_Chang_report_010615.pdf?mtime=20160906082142 (describing how the Chinese Communist Party uses national security to justify control over major elements of policymaking).

But, standing in the way of accomplishing these objectives is a power struggle between the various ministries in charge of regulating cyberspace.[58] Among them are the Ministry for Public Security, the National Bureau for State Secrets, the Ministry for Industry and Informatiziation, and the General Staff Division of the People's Liberation Army.[59] These ministries have chafed against one another due to the ambiguity of their authority over cyberspace, and the fact that the law grants the departments very broad, discretionary authority.[60] Recently, the creation of the "Central Cyber Security and Informatization Leading Group" (Leading Group) which, while lacking executive authority, was developed with the intention of creating a buffer between the various departments.[61]

At the heart of China's cybersecurity policy—even today, though it is now modified by the 2016 Cybersecurity Law—is the Multi-Level Protection Scheme (MLPS).[62] The scheme divides all potential Internet users among five different levels, with private individuals and small companies at the bottom (levels one and two), and public authorities at the top (level five).[63] To sell IT products to these parties, the product must meet certain criteria appropriate for that party's level.[64] For example, a level three IT product (to be sold to businesses in a strategically important sector, like finance) must:

(1) have been developed by Chinese citizens, legal entities, or companies with state participation;
(2) have the intellectual property for its key components owned by China;
(3) have been made by persons with no criminal record at all;
(4) contain no back doors or Trojan horses built in;
(5) pose no risk to national security, public order, or public interests; and
(6) be certified for requirements of national security.[65]

This means that companies like Microsoft are completely barred from selling their products to any party in China that qualifies as level three or above on the MLPS.[66] These protectionist policies can be considered reasonable from the Chinese perspective because such policies ensure the cybersecurity systems used in critical sectors are under the government's strict control.[67] There

58. *Digital Divide*, *supra* note 37, at 164–65; *see* Gierow, *supra* note 54, at 2–3.

59. Gierow, *supra* note 54, at 4.

60. *Digital Divide*, *supra* note 37, at 164–65; Gierow, *supra* note 54, at 2–3.

61. Gierow, *supra* note 54, at 3.

62. *Id.* at 5.

63. *Id.*

64. *Digital Divide*, *supra* note 37, at 161–62; Gierow, *supra* note 54, at 5.

65. Gierow, *supra* note 54, at 5.

66. *Id.* at 5.

67. *Id.* at 6.

are also obvious benefits of such a policy on local manufacturers.[68] Such a protectionist approach is also not unique to China, for example, the United States has been exercising a similar policy to prevent federal authorities from acquiring Chinese IT products.[69]

When foreign companies attempted to interact with the Chinese public via the Internet, the Chinese government enforced most of its measures through licensing arrangements with each foreign company.[70] A requirement to assist in censoring content offensive to the government was standard fare in these licensing arrangements, with companies towing the line under threat of their operations being banned from the country.[71]

Entering 20l6, the Chinese cybersecurity scheme was beginning to crystalize.[72] But even with a figurehead at the top in the form of the Leading Group, the various ministries worked at cross purposes as each tried to stretch the outer limits of their authority.[73]

B. The 2016 Cybersecurity Law

The first chapter of the new legislation states the intended purposes of the law, and broadly states who is entitled to the rights and obligations the law creates.[74] Some of the notable purposes of the law are advocating the dissemination of "core socialist values,"[75] and putting responsibility for planning, coordinating, supervising, and managing network security on government departments.[76] The chapter also puts the responsibility on individuals and organizations to report conduct endangering network security alongside an obligation on state departments to respond promptly.[77] There is also a mandate on "relevant network industry organizations" to strengthen their own security measure, without providing any scheme of how to accomplish

68. *Id.* at 7.

69. *Id.*

70. 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/ (citing Rebecca MacKinnon, *China's Censorship 2.0: How Companies Censor Bloggers*, FIRST MONDAY (Feb. 2, 2009), http://firstmonday.org/article/view/2378/2089).

71. *Id.*

72. *See generally Cybersecurity Law*, *supra* note 6.

73. Gierow, *supra* note 54, at 2–3.

74. *See Cybersecurity Law*, *supra* note 6, ch. 1.

75. *Id.* art. 6.

76. *Id.* art. 8.

77. *Id.* art. 14.

the mandate.[78] Of special note here is Article 12, which requires all persons and organizations to take no action that would risk harming China's socialist policies.[79]

Chapter two of the statute gives a general outline of how the government will carry out the strengthening of cybersecurity.[80] There is a mandate that all levels of government, from the State Council to autonomous regions and directly governed municipalities, make comprehensive plans to further several key sectors.[81] The State also claims to encourage several vectors of enhancing cybersecurity, like encouraging the innovation of new security technologies, supporting cybersecurity-related education in schools of higher learning or vocational schools, and otherwise seeking to "cultivate talent" in cybersecurity.[82]

In chapter three, the statute specifically outlines the requirements for network operators, those who manage services available on the Internet.[83] Here, the law states both general requirements that network operators must adhere to,[84] along with special duties for operators of "critical information

78. *Id.* art. 11.

79. *Cybersecurity Law*, *supra* note 6, art. 12 ("Any person and organization using networks shall abide by the Constitution and laws, observe public order and respect social morality; they must not endanger network security, and must not use the network to engage in activities endangering national security, national honor and interests, inciting subversion of national sovereignty, the overturn of the socialist system, inciting separatism, 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, as well as infringing on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts.").

80. *See id.* ch. 2.

81. *Id.* art. 16 ("[E]xpand their input; support key network security technology industries and programs; support network security technology research and development, application and popularization; spread safe and trustworthy network products and services; protect the intellectual property rights for network technologies; and support research and development institutions, schools of higher learning, and so forth to participate in State network security technology innovation programs.").

82. *Id.* art. 20.

83. *Id.* art. 76(3) (defining network operators); *see Cybersecurity Law*, *supra* note 6, ch. 3.

84. *See Cybersecurity Law*, *supra* note 6, art. 21 ("(1) Formulate internal security management systems and operating rules, determine persons responsible for network security, and implement network security protection responsibility; (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 sta-

infrastructure," which concerns what has been previously defined as CI.[85] Of special note here is the requirement for all network operators providing services like network access and information publication to obtain and store the real identity of the user.[86] CI network operators must also adhere to security plans that the relevant government departments will implement specifically on their industry.[87] But, what falls under the umbrella of CI as defined by this law is extraordinarily broad.[88] Typical areas are included, like power, water, and finance, but CI is also considered to be any area where the loss or leak of data "might seriously endanger national security, national welfare and the people's livelihood, or the public interest, on the basis of their tiered protection system."[89] The government also encourages network operators that do not manage CI to participate in the duties the law forces upon the CI network operators.[90] This is important because CI network operators must also submit themselves to review by relevant state departments when they seek to purchase network products and services that "might" impact their security.[91] Those CI operators must also physically store the data gathered or produced by operations within the country to the mainland territory of China, and must pass a security assessment from the government if it is truly necessary to

tuses and network security incidents, and follow relevant provisions to store network logs for at least six months; (4) Adopt measures such as data classification, back-up of important data, and encryption; (5) Other obligations provided by law or administrative regulations.").

85. *Id.* art. 34 ("(1) Set up specialized security management bodies and persons responsible for security management, and conduct security background checks on those responsible persons and personnel in critical positions; (2) Periodically conduct network security education, technical training and skills evaluations for employees; (3) Conduct disaster recovery backups of important systems and databases; (4) Formulate emergency response plans for network security incidents, and periodically organize drills; (5) Other obligations provided by law or administrative regulations.").

86. *Id.* art. 24 ("Network operators handling network access and domain registration services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services, shall require users to provide real identity information when signing agreements with users or confirming provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services. The State implements a network identity credibility strategy, and supports research and development of secure and convenient electronic identity confirmation technologies, promoting reciprocal acceptance among different electronic identity confirmations.").

87. *Cybersecurity Law*, *supra* note 6, art. 32.

88. *See id.* art. 31.

89. *Id.*

90. *Id.*

91. *Cybersecurity Law*, *supra* note 6, art. 35.

provide the data outside the border.[92] Altogether, CI network operators must submit to heavy state supervision and scrutiny that frequently involves revealing sensitive data to the government.[93]

Chapter four goes into greater detail on the requirements of standard network operators (not dealing with CI).[94] Most of the chapter devotes itself to entailing what lengths must be reached to ensure the confidentially of what limited personal information the network operator collects to provide its services.[95] This is relevant due to the requirement that only real identities may be provided when an individual solicits network access, domain registration, or information publication services.[96] Another article of note is a mandate that the network operators manage information published by user, requiring that the operator prevent the publication of any information that is prohibited by administrative regulations or other laws.[97] This effectively conscripts network operators into furthering the government's censorship policies and public monitoring, as the operator is required to report the attempt to publish the information to "relevant competent departments."[98] Network operators must also submit to general state supervision and management.[99]

Chapter five deals with how the state departments will monitor cybersecurity efforts, alongside what the departments are required to plan for in terms of if a security risk is identified.[100] The last article of the chapter is noteworthy as it empowers the State Council, along with other levels of government with the State Council's approval, to take temporary measures to control network communications in response to emergencies or production

92. *Id.* art. 37.

93. *Id.* art. 39 ("State network information departments shall coordinate relevant departments in employing the following measures for critical information infrastructure security protection: (1) Conduct spot testing of critical information infrastructure security risks, put forward improvement measures, and when necessary may retain a network security service establishment to conduct testing and assessment of network security risks. (2) Periodically organize critical information infrastructure operators to conduct emergency network security response drills, increasing the level, coordination, and capacity of responses to network security incidents. (3) Promote network security information sharing among relevant departments, critical information infrastructure operators, and also relevant research institutions, network security services establishments. (4) Provide technical support and assistance for network security emergency management and recovery and so forth.").

94. *See id.* ch. 4.

95. *Id.* arts. 40–45.

96. *Id.* art. 24.

97. *Cybersecurity Law*, *supra* note 6, art. 47.

98. *Id.* art. 47.

99. *Id.* art. 50.

100. *See id.* ch. 5.

safety accidents.[101] Among the permitted measures is outright restriction of access.[102]

Chapter six discusses liability for network operators who are found to be violating this statute.[103] Of special note is the fact that the government targets individuals and management directly responsible for the violation with the appropriate fine, instead of putting the fine on the larger business.[104] Another couple of articles make the furthering of state censorship clear, with the failure to prevent the dissemination of prohibited information being a fine and a suspension of operations.[105] Article 70 expands the scope of prohibited information by including Article 12 (the requirement that no one use the Internet to disturb "core socialist values") in the realm of punishable violations.[106]

The 2016 Cybersecurity Law appears to be both strict and vague. While duties are specified and penalties detailed, much is left up to the relevant departments to create.[107] This does little to solve the problem of the inter-ministry struggles that characterized the regime up to this point.[108] At the same time, it is clear that China intends to press gang network operators into furthering its censorship, even going as far as to have the operators act like state-sponsored spies.[109] While some could consider this little more than a codification of previously informal practices, the adoption of such a framework cements China as an authoritarian regime maintaining a tight grip on everything its citizens see and hear.[110] This is a clear sign that the country wants to approach cybersecurity with a paternalistic approach, even if the law pays lip service to an international effort to secure cyberspace.[111]

IV. A COMPARISON OF CYBERSECURITY REGIMES

To better provide context for where China sits in the spectrum of government control, this Part concerns itself with an overview of the various cybersecurity regimes implemented in other countries. These countries have

101. *Id.* art. 58.

102. *Id.*

103. *See Cybersecurity Law*, *supra* note 6, ch. 6.

104. *Id.* art. 60.

105. *Id.* arts. 68–69.

106. *Id.* art. 70.

107. *See id.* arts. 8, 19, 23, 39, 49, 50, 51, 53, 69(1) (detailing what various plans and operations are left to the discretion of "relevant departments").

108. Gierow, *supra* note 54, at 2, 4.

109. *Cybersecurity Law*, *supra* note 6, art. 50; *see also id*. art. 12.

110. Bethany Allen-Ebrahimian, *The 'Chilling Effect' of China's New Cybersecurity Regime*, Foreign Policy (Jul. 10, 2015), http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-Internet-security/.

111. *See Digital Divide*, *supra* note 37, at 121.

been selected because of their geographic, political, and technological position in the world, as all appear to play a role in shaping each countries' cybersecurity regimes. This comparison should show that while every countries' regime has its own unique approach to the same issues, there are general trends that can be associated with certain political and geographic relationships.

A. The Current Regimes

1. United States

While the United States is not the most "wired" country (that honor goes to South Korea), nor the most "free" country online (recognized to be Estonia), its position as a superpower and advocate of influential cybersecurity policy makes it impossible to leave out of such a comparative analysis.[112] The United States may indulge in some hypocrisy, especially in light of the NSA scandal,[113] but its support for free expression and the free flow of information online puts at a stark contrast of the blatant censorship and authoritarian top-down cybersecurity regime of China.[114]

In the United States, the regime is a mix between statutory requirements, common law duties (e.g., negligence and corporate fiduciaries) and a multi-stakeholder framework for private companies to look at as a model of improve their own networks.[115] In its statutory requirements, the United States uses a sectoral approach, where the laws are drafted for a specific industry.[116] Unfortunately, the execution of these broad statutes has been hindered by a fragmented bureaucracy.[117] There also are security regulations

112. Shackelford, *Toward Cyberpeace*, *supra* note 10, at 1310–11.

113. Funk, *supra* note 28, at 50–51.

114. *See id.* at 55.

115. Scott J. Shackelford et al., *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217, 223 (2016); *see also* Shackelford et al., *Toward a Global Cybersecurity Standard of Care?*, *supra* note 51, at 311–25 (discussing the various aspects of the United States' cybersecurity regime).

116. *See* Shackelford et al., *Toward a Global Cybersecurity Standard of Care?*, *supra* note 51, at 321. Examples of such sectorial legislation include the following: the Gramm-Leach-Bliley Act for the financial sector; the Chemical Facility Anti-Terrorism Standards Regulation for the chemical sector; the Health Insurance Portability and Accountability Act for the public health sector; and the North American Electric Reliability Corporation Standards for the energy sector. *See id.* at 321–25.

117. Shackelford et al., *Bottoms Up*, *supra* note 115, at 221 ("Still, a single, comprehensive approach to U.S. cybersecurity law and policy has yet to emerge with a veritable alphabet soup of agencies, including the Department of Homeland Security, NSA, and the Federal Trade Commission, responsible for various aspects of the nation's cyber defense; the Department of Defense alone report-

effective in most of the individual states.[118] But, since these laws vary from state to state, this has created a complex and contradictory entanglement of regulations.[119]

The National Institute for Standards and Technology (NIST) was given the task of developing a framework that companies could use to map out their current level of readiness regarding cyberattacks, and what was required to improve that readiness.[120] It is also now being considered in some areas to be a possible standard of due diligence.[121] The Framework's most interesting feature is its use as a common language for entities involved in cyber infrastructure to evaluate their current posture, determine a targeted state, and assess their progress towards that targeted state.[122] It operates through a process that utilizes three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile.[123] The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes.[124] It is a non-exhaustive list of industry-specific best practices for managing cyber risk and uses a common terminology that allows for organizations to communicate more effectively.[125] These practices are sorted into Informative References, which are placed at the bottom of a sorting hierarchy, from Function, to Categories, to Subcategories, and finally to the Informative References.[126] The Framework

edly operates more than 15,000 networks in 4,000 installations spread across 88 countries.").

118. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?*, *supra* note 51, at 325–26.

119. *Id.* at 325 ("[F]or example, a handful of states have a 'no-harm threshold law,' meaning that it does not matter whether lost information was used in a way that harmed consumers or not—the mere fact that there has been a breach requires that notification be given. States also have more-or-less-inclusive lists of personally identifiable information that must be lost for a breach to warrant disclosure. Meanwhile, in the states that do not have any data breach notification laws as of 2014—Alabama, South Dakota, and New Mexico—a company could knowingly have its customers' social security numbers breached but not inform those customers and still be legally compliant under state law.").

120. Shackelford et al., *Bottoms Up*, *supra* note 115, at 221.

121. *Id.* at 222.

122. *Id.* at 223.

123. *Id.*

124. *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH. 4–5 (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf [hereinafter *NIST Framework*].

125. Shackelford et al., *Bottoms Up*, *supra* note 115, at 224.

126. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?*, *supra* note 51, at 330–31 ("For example, the 'Identify' Function contains within it the

Implementation Tiers are four progressive levels (Partial, Risk Informed, Repeatable, and Adaptive) that illustrate how well a firm manages cyber risk with their Enterprise Risk Management (ERM) practices as compared to the best practices listed in the Framework Core.[127] Taking into account those practices, the current cyber threat environment, regulatory requirements, business objectives, and organization constraints, a firm should be able to identify which tier it belongs to.[128] Further illustrating the Framework's Core Functions and Categories are the Framework Profiles, which allow a firm to recognize gaps in their governance of cybersecurity that need to be addressed before it can reach its cyber risk management objectives.[129] It does so by using the information gathered from the Core and the Tiers, identifying its current Profile and its target Profile, and determining what needs to be addressed to achieve its target Profile from where it differs from the current Profile.[130]

The NIST Framework is adaptable, and can expand globally because of its reference to standards recognized worldwide as best practices.[131] Because of this, it has the potential to serve as a model for international cybersecurity regulation.[132] But, it not a flawless system. Its spread relies entirely on its appeal to individual businesses, and any sort of recognizable standard that can serve as a matter of law will take time to develop.[133] Even when it does, scholars argue it may "not go far enough in scope, influence, or impact."[134]

'Asset Management' Category, which articulates practice outcomes to identify and manage the 'data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes . . . consistent with their relative importance to business objectives and the organization's risk strategy.' ").

127. Shackelford et al., *Bottoms Up*, *supra* note 115, at 225.

128. *Id.*

129. *Id.*

130. *Id.* (citing *NIST Framework*, *supra* note 124, at 4).

131. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?*, *supra* note 51, at 336–37.

132. *Id.*

133. *See* Shackelford et al., *Bottoms Up*, *supra* note 115, at 225–26.

134. Scott J. Shackelford, *Protecting Intellectual Property and Privacy in The Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk*, 19 CHAP. L. REV. 445, 460 (2016) (citing Tony Romm, *Cybersecurity Still in Slow Lane*, POLITICO (Feb. 9, 2014, 10:40 PM), http://www.politico.com/story/2014/02/cybersecurity-in-slow-lane-one-year-after-obama-order-103307.html?hp=f1).

2. United Kingdom

The United Kingdom (UK) is moving towards a NIST Framework, but has not adopted the structure fully.[135] Generally, the UK has focused on developing voluntary standards to enhance CI security.[136] In 2014, it took another step in this direction with the "Cyber Essentials" program, created to "incentivize widespread adoption of basic security controls that will help to protect organizations against the commonest kind of attack."[137] A certification program, Cyber Essentials was made mandatory for all UK government contractors handling personal or sensitive information, but is voluntary to all others.[138] Cyber Essentials' requirements include self-certification for basic security systems, like firewalls, secured configuration, user access control, and patch management.[139] The Cyber Essentials Assurance Framework is going to supplement existing organizational approaches to risk management.[140] Specifically, the certification requirements call on businesses to follow the British government's "Ten Steps to Cyber Security."[141]

In 2015, the Advice Sheets were added to the ten-step cybersecurity program.[142] They set out the actions and measures that represent a good foundation for effective information risk management, much like the NIST Framework, but without the extensive categorization.[143] While the structure is not copied, many of the objectives listed in the NIST Framework's Categories and Subcategories have been adopted by the Advice Sheets.[144] Since the release of the 2015 Advice Sheets coincided with a joint announcement between the chief executives of the United States and the UK proclaiming an

135. Shackelford et al., *Bottoms Up*, *supra* note 115, at 229–30.

136. *Id.* at 228.

137. *Id.*

138. *Id.*

139. *Id.* (citing U.K. Dep't for Bus., Innovation & Skills, Cyber Essentials Scheme Requirements (June 2014), http://www.cyberstreetwise.com/cyberessentials/files/requirements.pdf.).

140. *Id.* (citing U.K. Dep't for Bus., Innovation & Skills, Cyber Essentials Scheme Assurance Framework (2015), http://www.cyberstreetwise.com/cyberessentials/files/assurance-framework.pdf.).

141. Shackelford et al., *Bottoms Up*, *supra* note 115, at 229 (citing U.K. Dep't for Bus., Innovation & Skills, Cybersecurity Guidance for Business (2015), https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility).

142. *Id.* at 229–30.

143. *Id.*

144. *Id.* at 230.

intent to work with industry to align cybersecurity best practices and standards, it appears to be a manifestation of that proclamation.[145]

3. European Union

Noteworthy at the outset of this section is the odd relationship the European Union (EU) has in both being a source of uniform regulations, and a collection of sovereign states that have the authority to implement state-specific solutions.[146] As a result, the organization has the more difficult task of achieving harmony among best practices in cybersecurity.[147] Regardless, the EU as a whole has recognized the importance of balancing security with free flow of data.[148] But, in contrast to the United States, the EU's approach to regulating cyberspace is comprehensive, with one cybersecurity law covering most industries and providing greater uniformity.[149] The current EU cybersecurity strategy has five priorities:

(1) achieving cyber resilience;
(2) reducing cybercrime;
(3) creating a new cyber defense policy;
(4) developing industrial and technological resources for cybersecurity; and
(5) establishing an international cyberspace policy for the European Union that promotes core EU values.[150]

To accomplish the first priority, there is emphasis on cooperation between the public and private sectors, along with propositions for minimal security requirements that would apply to all Member States.[151] For the second priority, the strategy is focused on combatting the use of botnets, networks of computers infected by a program which coordinates them to attack servers by overloading them with requests.[152] The cyber defense policy is the result of

145. *Id.* at 230–31 (citing *FACT SHEET: U.S.-United Kingdom Cybersecurity Cooperation*, Office of the Press Sec'y (2015), https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation).

146. Shackelford et al., *Bottoms Up*, *supra* note 115, at 237.

147. *Id.*

148. *See* Chander & Le, *supra* note 46, at 688 (citing Council Directive 95/46, 1995 O.J. (L 281) 31, 36–37).

149. Kenneth K. Dort et al., Cyberspace Law: Recent Trends in the United States and the European Union (2015).

150. *Digital Divide*, *supra* note 37, at 156 (citing *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, at 4–5 JOIN (2013) 1 final (Feb. 7, 2013)).

151. *Id.*

152. *Id.* at 157.

collaboration between civilian and military approaches in protecting critical cyber assets.[153] Finally, the EU seeks to "promote openness and freedom on the Internet, close the digital divide, and build consensus in international cybersecurity policymaking."[154]

The EU has undergone some localization policies, mainly codified by the General Data Protection Regulation (GDPR).[155] The GDPR allows companies to transfer data outside the EU if appropriate safeguards are in place, such as binding corporate rules, a valid "European Data Protection Seal" for both controller and recipient, standard data protection clauses, or contractual clauses with prior authorization from the member state's data protection authority.[156] Originally, there was a safe harbor provision for the United States, allowing for the transfer of data without certification so long as certain protection standards were met. This provision has since transformed into the 2016 US-EU Privacy Shield.[157]

4. Russia

The Russian government has adopted many of the measures taken by China to ensure its cybersecurity.[158] Some of this is the result of sanctions from the West, preventing Russia from using Western technology to carry out its localization policies.[159] The government has sought to localize data by prohibiting the storage of Russians' personal data outside the country.[160] The locations of the storage facilities must also be disclosed to the government.[161] Any entity that organizes the dissemination of information on the Internet is required to store all information about the arrival, transmission, delivery, and processing of voice data, written text, images, sounds, or other kinds of action for six months in Russia.[162] Legislation was passed near the end of 2016 that effectively gives the government control over much of the physical ar-

153. *Id.*

154. *Id.*

155. Chander & Le, *supra* note 46, at 690.

156. *Id.*

157. *See generally* European Commission Press Release IP/16/216, EU Commission and United States Agree on a New Framework for Transatlantic Data Flows: EU-US Privacy Shield (Feb. 2, 2016) (detailing the new arrangement for the migration of data between the European Union and United States).

158. Andrei Soldatov & Trina Borogan, *Putin Brings China's Great Firewall to Russia in Cybersecurity Pact*, The Guardian (Nov. 29, 2016, 2:00 AM), https://www.theguardian.com/world/2016/nov/29/putin-china-Internet-great-firewall-russia-cybersecurity-pact.

159. *Id.*

160. Chander & Le, *supra* note 46, at 701.

161. *Id.* at 702.

162. *See* Shackelford et al., *Bottoms Up*, *supra* note 115, at 229–30.

chitecture of the Internet in the country, from exchange points to domain names and cross-border fiber-optic cables.[163]

5. Israel

Frequently attacked by both private and state actors, Israel has developed what is widely recognized as one of the most sophisticated cybersecurity systems in the world.[164] The cybersecurity regime is focused on the efforts of the Israel National Cyber Bureau (INCB), whose purpose is threefold: to defend national infrastructures from cyberattack; advance Israel as a world-leading center of information technology; and encourage cooperation between academia, industry, and the private sector, as well as between government agencies and the security community.[165] The INCB categorizes projects to accomplish its mandate into three areas: the development of cybersecurity infrastructure, the organization of personnel concerning that effort, and the maintenance of a cybersecurity network.[166] Two of the accomplished projects thus far are coordinating between government ministries to foster both academic and entrepreneurial research and the development of cybersecurity products.[167] The third and latest project was a more direct approach towards academic research, partnering with two Israeli universities to research not only technology, but also relationships between technology, social science, and legal fields.[168] At the same time, the organization also consolidated the administrative aspects of cyber regulation and made recommendations to the government through a multi-stakeholder process.[169] Overall, the Israeli approach seems to be an almost even split between direct government control and allowing other stakeholders to lead the charge, as it is a government agency that both directs and promotes cybersecurity. This is

163. *Id.*

164. Daniel Benoliel, *Towards A Cybersecurity Policy Model: Israel National Cyber Bureau Case Study*, 16 N.C. J.L. & TECH. 435, 442 (2015).

165. *Id.* at 443 (citing Advancing National Cyberspace Capabilities, Res. No. 3611 (2011), http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf) (Isr.).

166. *Id.* at 443–44.

167. *Id.* at 448–49.

168. *Id.* at 449.

169. *Id.* at 451; *see also id.* at 451 n.78 ("The process included four stages. Initially, INCB collected and processed expert testimonies. Soon after, a public advisory committee was established. Then a series of open consultations as well as particular consultations took place. Lastly, INCB generated a list of recommendations, which were at first open for public commentary, and then the INCB passed the final regulation recommendations to the Israeli government for consideration.").

especially shown in the INCB's strategy in establishing a regulatory framework.[170]

6. India

India has been slow to adopt a cybersecurity regime, and what it has now could be recognized as one still in infancy.[171] The Indian IT Act of 2000 appears to serve as the foundation for the current cybersecurity regime.[172] Amended in 2006 to require protection of what the law identified as "Critical Information Infrastructure," it made companies liable if they did not follow "reasonable security practices and procedures."[173] Amended again in 2008, the law made companies liable if they were negligent in implementing and maintaining reasonable security practices, with said practices defined by either a specific agreement between the parties, by law, or "by the Central Government in consultation with such professional bodies or associations as it may deem fit."[174] This resulted in the Indian government having broad authority to dictate what measures were required to ensure CI protection.[175] In trying to secure its citizen's data, India has implemented a localization policy, preventing transfers of data abroad unless it is for the "necessary" end of a contract.[176] The country also has demonstrated the desire to locally develop technologies that can help protect CI and enable economic development, as shown by the 2013 National Cyber Security Policy.[177]

---

170. Benoliel, *supra* note 164, at 451 ("The first strategic proposition solicits recommendations 'to the Prime Minister and government regarding national cyber policy.' The second and third propositions are more general and thematic: to 'promote research and development in cyberspace and supercomputing,' and to devise a 'national concept' for coping with 'emergency situations in cyberspace.' ").

171. *Digital Divide*, *supra* note 37, at 165.

172. *Id.* at 166.

173. *Id.*

174. *Id.*

175. *Id.*

176. Chander & Le, *supra* note 46, at 695 (quoting Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, subsec. II(3)(i) (Apr. 11, 2011)). ("A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. *The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer*.") (emphasis added).

177. *Digital Divide*, *supra* note 37, at 168.

While it initially appears that India is emulating the "Internet Sovereignty" policies of Russia and China, the 2013 policy also gave individual businesses the capacity to structure their own security program, emulating the "bottom-up" approach used in Europe and the United States.[178] India has also made strides to try and promote internationally recognized best practices by promulgating guidelines through its National Critical Information Infrastructure Protection Centre.[179]

7. Japan

Japan faces a similar threat in cyberspace as the United States and the EU, and similarly favors self-governance for the private sector over top-down legislation.[180] The 2015 strategy for the country emphasizes that "Autonomy" and "Collaboration among Multistakeholders" are core principles that inform the entire strategy.[181] The government combined that philosophy with a scheme much like the NIST Framework, providing a guiding framework that "enables stakeholders . . . to promptly evaluate enterprises' efforts to address cybersecurity."[182] If a firm makes an effort to follow the framework to evaluate and enhance their cybersecurity, financial incentives are provided.[183] The end result is a mix of self-governance for the private sector and regulatory oversight, portraying the role of government as a policy emphasizer that encourages the private sector to motivate itself and take their own initiatives.[184] The current strategy also specifies "security by design," making cybersecurity considerations central to the development process of new products.[185] Since any relevant products are the result of the input of multiple stakeholders, the strategy promotes a dialogue in these areas.[186] It does so by first assessing the benefits and risks of potential policies and then setting forth security obligations for the various stakeholders.[187] So the Japanese approach appears to prefer private action over state rule, but seeks to foster such initiative by taking the first steps alongside the private sector.[188]

178. *Id.*

179. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?*, *supra* note 51, at 350.

180. *Id.* at 242.

181. *Id.* at 244 (quoting *Cybersecurity Strategy*, GOV'T OF JAPAN (Sept. 4, 2015), http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf).

182. *Id.*

183. *Id.*

184. *Id.*

185. Shackelford et al., *Bottoms Up*, *supra* note 115, at 244.

186. *Id.* at 245.

187. *Id.*

188. *See id.*

8. South Korea

Unlike Japan and the United States, South Korea has used a heavier hand when dictating cybersecurity policy.[189] Frequently the target of attacks from North Korea, South Korea has instituted both broad-spectrum protections of personal data along with sectoral regulations governing other areas of cybersecurity.[190] Specifically, there is the Personal Information Protection Act, which regulates the collection and use of personal information—most importantly, resident registration numbers, which are similar to Social Security Numbers in the United States—and requires a minimum of cybersecurity precautions.[191] Breach notifications are also part of the regime, keeping the government aware of any leaks in the system.[192]

South Korea also practices localization policies from both modern and decades-old statutes. While data is allowed to be exported, the manager of the information of the "data subject" (the original collector of a person's data), must provide extensive information about the overseas transfer to the data subject.[193] Another, more obscure source of localization is the 1961 Land Survey Act (replaced in 2009 by the Act on Land Survey), which is primarily used to prevent mapping data of the country from being stored on servers outside the country.[194]

9. Summary

There are geographic and political factors guiding the decision on how to handle cybersecurity in these countries. The more authoritative regimes, Russia and China, aim towards a nationalistic approach, with their respective governments solidly helming all action and supervising as much of the network as they can.[195] Such a policy helps them stifle political dissent within their regulated networks.[196] Meanwhile, Europe and the United States take a more cooperative stance with the private sector, not precisely treating the net as a "commons," but working collaboratively to create something that could be recognized as a standard of care for cybersecurity.[197] At the same time, smaller countries tend to gravitate towards whatever larger power (e.g., Rus-

189. *Id.* at 246.

190. *Id.*

191. Shackelford et al., *Bottoms Up*, *supra* note 115, at 246.

192. *Id.* at 245.

193. Chander & Le, *supra* note 46, at 703–04.

194. *Id.* at 704.

195. *See* Eichensehr, *supra* note 52, at 331.

196. *Id.*

197. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?*, *supra* note 51, at 309–311, 346.

sia, China, United States), exerts greater influence upon them.[198] For example, while South Korea tries to emulate western policies, it proximity to China and the threat its faces from an aggressive North Korea force it to take more of a middle path between protecting its "borders" in cyberspace and joining the commons.[199]

B. The Potential Harms of China's Cybersecurity Regime

China's cybersecurity law could inflict far-reaching harm. The country's economic ties and massive domestic market of over a billion consumers makes it a difficult entity to negotiate with. Few companies will be able to avoid adhering to this law and remain competitive in the global market. The potential harms of China's cybersecurity regime thus include both (1) a negative effect on the Chinese people and (2) foreign companies seeking profit in China.

1. Harm to the Chinese Public

The most obvious harm is the expansion of the authoritarian state, which seeks to deprive its citizens of information that it deems would harm its own power. This is a hallmark of an authoritarian regime, to silence dissent within and prevent access to subversive information without. Thus, the public's ability to express itself is sorely diminished, while at the same time society as a whole receives little to no benefit.

Regarding the typical, benign motives that the government has set forth, such as trying to protect the privacy of the public and safeguarding infrastructure from attack or surveillance, such a policy appears to contravene those ends rather than achieve them.[200] First, the law actively works against any preservation of privacy alone, forcing citizens to present their real identity to network operators. This allows for the government to indirectly monitor, without due process, citizen's online activities. This is a blatant scheme that puts the party in place of the government, allowing it to quickly stifle dissent. The localization requirement will also most likely make Chinese data even easier to attack, as not only will the technology in China fall behind (discussed in more detail below), but the fact that all the data is bound within the borders of the country means that the public loses out on the global distribution of data across servers.[201] This saves foreign surveillance operations in logistical costs, as they can concentrate their efforts on specific locations.[202] Private actors also see these policies as inherently weak, since other countries

198. *See* Shackelford et al., *Bottoms Up*, *supra* note 115 at 242–43, 247–48; *see also* Eichensehr, *supra* note 52, at 335.

199. Shackelford et al., *Bottoms Up*, *supra* note 115, at 247–48.

200. Chander & Le, *supra* note 46, at 715.

201. *Id.* at 716–717 (known as the "Protected Local Provider" problem).

202. *Id.* (this is called the "Jackpot" problem).

that have implemented localization policies, like Vietnam and Indonesia, have become massive targets for hackers.[203]

Even when taking into consideration China's stated economic goals for such a regime, the public will most likely be unable to reap the benefits. China's intentions for its cybersecurity policy is to improve security and foster a domestic market for demand and innovation.[204] But, it is unlikely this regime will achieve those ends. First, with regards to fostering domestic innovation, depriving the Chinese market of competition from abroad actively works against that goal. Much like protectionist policies regarding trade, a decline in competition stagnates development, as domestic producers no longer need to keep up with foreign producers to sustain themselves. As technology enhancing cybersecurity advances, the Chinese will most likely be left with inferior products from domestic producers, and as a result could be even more vulnerable to attacks.[205] It is arguable that the domestic product is either already inferior or is simply nonexistent, as China has been a net importer of technology.[206] In fact, most of the technology the Chinese government uses to censor the public's access to the Internet comes from American IT companies.[207] Second, China's hope to grow the domestic economy by requiring storage of data to be within the borders of the country will also fail to provide any cognizable benefit for the public, because such a policy has been seen to only benefit a small group of people and enterprises.[208] Only the companies that manage or service very expensive data centers will see any benefit, and these companies do not require many employees because data centers are more power-intensive than workforce-intensive.[209] Meanwhile, the localization policy will be widely felt by businesses of any size that are denied access to global services they might use improve productivity.[210] At the same time, domestic start-ups will be denied access to cheaper data centers abroad, most likely stalling any effort to start the business in the first place.[211] This effect can hurt even businesses not specifically tied to the In-

203. *Id.* at 720–721.

204. *See Digital Divide*, *supra* note 37, at 162–63.

205. *See* Chander & Le, *supra* note 46, at 715–18.

206. Richard Winfield & Kristin Mendoza, *Does China Hope to Remap The Internet in Its Own Image?*, 2 J. Int'l Media & Ent. L. 85, 93 (2008).

207. *Id.*

208. *See* Chander & Le, *supra* note 46, at 722–23.

209. *Id.* at 724.

210. *Id.* at 722–23. ("For example, besides the loss of international social media platforms, localization would make it impossible for Russians to order airline tickets or consumer goods through online services. Localization requirements also seriously affect Russian companies like Aeroflot because the airline depends on foreign ticket-booking systems.").

211. *Id.* at 725.

ternet, as it has been seen that most of the economic benefits of Internet technologies end up in traditional businesses like agriculture and healthcare.[212]

Another factor of this law that will hinder economic growth is the amount of discretionary authority it gives the various (and overlapping) state ministries.[213] In allowing each ministry to sculpt its own regulatory landscape, each individual area of business will have to deal with disparate, and perhaps even conflicting, legislation.[214] Meanwhile, the turf battles between the ministries could also freeze up the regulatory process.[215] Ultimately, this law will most likely fail to provide the Chinese with the benefits that the government has stated as their objectives. At the same time, the public will most likely be harmed, not only by the cost of implementing this law and the possible loss of access to larger portions of the Internet, but also by the economic losses that will result when foreign businesses are forced to react to the burdens of the new legislation. Such burdens are discussed below.

2. Harm to Foreign Businesses

Many foreign companies and economic conglomerates petitioned the Chinese government to not enact this law as it was being drafted.[216] This was for good reason, as this law has an onerous effect on any company that wants access to the Chinese market. Combining that with the fact that the Chinese market counts for roughly a seventh of the global population means that almost any company with international reach will either suffer additional costs and strict government oversight or lose out on accessing the single biggest

212. *Id.* at 727 (citing James Manyika et al., *Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy*, McKinsey Global Inst. 55 (2013), http://www.mckinsey.com/insights/business_technology/disruptive_technologies). ("The potential economic impact across the major sectors—healthcare, manufacturing, electricity, urban infra-structure, security, agriculture, retail, etc.—is estimated at $2.7 to $6.2 trillion per year.").

213. *See Cybersecurity Law*, *supra* note 6, art. 8; *see also Digital Divide*, *supra* note 37, at 164–65.

214. *See Cybersecurity Law*, *supra* note 6, art. 8, 32; *see also Digital Divide*, *supra* note 37, at 164–65.

215. *See Digital Divide*, *supra* note 37, at 165; *see also* Allen-Ebrahimian, *supra* note 110.

216. *China Adopts Tough Cyber-Security Law*, Economist (Nov. 12, 2016), http://www.economist.com/news/china/21710001-foreign-firms-are-worried-china-adopts-tough-cyber-security-law; Katie 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/; Sue-Lin Wong & Michael Martina, *China Adopts Cyber Security Law in Face of Overseas Opposition*, Reuters (Nov. 7, 2016 4:49 AM), http://www.reuters.com/article/us-china-parliament-cyber-idUSKBN132049; Allen-Ebrahimian, *supra* note 110; Ruan, *supra* note 70.

market on the planet.[217] After this law becomes effective, companies wishing to enter the Chinese market will not only have to weigh the cost of handling user data within the country and opening up their business to government oversight, but will also need to settle the ethical question of whether the company can be complicit in helping the government monitor the activities of its citizens.[218] Of course, motivated by the typical desire to maximize profit, most companies would comply, succumbing to what is a thinly disguised case of economic blackmail.[219]

A good illustration of the trouble foreign business needs to endure to access the Chinese market is Google's attempt to establish a Chinese domain (google.cn). Google, known for its informal maxim "don't be evil,"[220] originally had difficulty accessing the Chinese market from operations based in California (a dot-com domain with Chinese translation), both because of the government filtering search results and outright outages.[221] Upon establishing a dot-cn domain, Google began to self-censor in accordance with Chinese regulations.[222] Google was aware that such a move ran counter to its policies, but decided that the good it could provide outweighed the harm of following the government's censorship scheme.[223] A few years later, after experiencing a massive cyberattack that appeared to be from a Chinese attempt to access the accounts of Chinese human rights activists, Google ceased its self-censorship and shifted its operations in China to Hong Kong (changing domains from ".cn" to ".hk").[224] This led to a return to the status quo before Google.cn was established, with the site facing frequent filtering in China.[225] But, a surprising result of the conflict was a renewal of Google's license to operate

217. *See* 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, 412–13 (2013).

218. *See id.* at 426–427.

219. *See id.* at 426.

220. *Id.* at 410.

221. *Id.* at 413.

222. *Id.* at 413–414. This appears to be the essence of the trap the Chinese government has created. It censors content from abroad (causing the service to slow down and become unreliable) to compel companies to develop local operations, at which point the company falls under the country's territorial laws and must self-censor. *See* Lee et al., *supra* note 217, at 425.

223. *Id.* at 414. ("The company admitted that its self-censorship 'runs counter to Google's most basic values and commitments.' According to Google's Chief Legal Officer, David Drummond, Google 'launched Google.cn . . . in the belief that the benefits of increased access to information for people in China and a more open Internet outweighed our discomfort in agreeing to censor some results.'").

224. *Id.* at 417–18.

225. *Id.* at 418.

as an Internet Content Provider, believed by some to be an attempt by the government to distance itself from the perception that the business market in the country was highly politicized.[226] Unfortunately, while some touted Google's move as a successful protest of the Chinese censorship policies, the ultimate result was the Chinese public being deprived of access to a wealth of information.[227]

Google had to deal with censorship regulations before the drafting of the law that concerns this comment. Under the new law, Google will most likely have to store user data (with the true identity of the user) and that data could easily be collected by the government.[228] Also, should a user have posted content the government found offensive on the company's social media application, Google+, or its Gmail service, the company would have to not only take the content down but may have been obligated to report it.[229] Such a scheme may not be entirely offensive if the content in question threatened violence, but under the Chinese government's policies as reflected in the 2016 Cybersecurity Law, this content could simply be something that offends the country's socialist policies.[230] Microsoft and Yahoo! proved this by their own actions, by shutting down those who create content that speaks out against the Chinese government and even going so far as to assist in their detention.[231]

Facing such a hostile and oppressive environment can lead to economic decline if companies decide they cannot, or will not, shoulder the burden. The chilling effect will likely send aftershocks through the global economy. Such a global impact is discussed in more detail below.

3. Harm to Globalization

Whether globalization itself is a positive force that should not be stymied is beyond the scope of this comment. This comment is only concerned with the impact the law will have on the globalization trend. Here the

226. *Id.* (citing Rebecca MacKinnon, *On Google's License Renewal and Principled Engagement*, RCONVERSATION (July 9, 2010), http://rconversation.blogs.com/rconversation/2010/07/on-googles-license-renewal-and-principled-engagement.html).

227. *Id.* at 423–24 (citing SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY) 118–19 (2011)).

228. *See Cybersecurity Law*, *supra* note 6, arts. 8, 9, 37, 50.

229. *See id.* arts. 47, 48, 68, 70.

230. *See* Allen-Ebrahimian, *supra* note 110.

231. Lee et al., *supra* note 217, at 415–16. It should be noted that Yahoo! later moved its storage facilities out of China to prevent incidents like these from recurring, however, should its services later be found to constitute critical infrastructure, the company would either have to return to storing the data in China or cease operating in the country altogether. *See* Cybersecurity Law, *supra* note 6, art. 37.

problem is two potential outcomes that are not mutually exclusive: (1) China so burdens access to its people online that it puts a noticeable drag on the growth of cloud-based businesses, slowing down economies that put an emphasis on that industry; and (2) China uses its connections within the global community to spread its cyber-protectionist policies, compounding the issues already discussed above.

As the Internet has grown, the possibilities of cyberspace have increased exponentially alongside it. But, as these possibilities are exploited, they become more dependent on interconnectivity being maintained. With its special position in the global economy, China can make big waves should it choose to complicate matters. Unfortunately, this is what the 2016 Cybersecurity Law appears to be leaning towards, as it seems to—despite having articles to the contrary[232]—try and isolate China from the rest of the Internet.[233] As previously discussed, the barrier China is trying to erect makes international commerce harder, as larger companies have to adjust their networks to accommodate the Cybersecurity Law, or miss out on reaching a massive market; both have economic costs that will naturally be passed onto the consumer.[234]

This drag on the global community would be multiplied should other countries began to adopt the burdens China puts on those attempting to access its citizens. As Peter Wu was quoted in *Who Controls the Internet?*, "the question is no longer how the Internet will affect China. It is how China will affect the Internet."[235] Already, Russia appears to be following down the road China has laid, and countries like South Korea and India appear to be torn between the United States and China, appearing to posture like the giants on the playground.[236] In fact, it appears that this could be a goal for China, to attempt to take the lead in dictating global Internet governance.[237] Should a scheme much like the one advanced by the 2016 Cybersecurity Law spread, the burdens it would place on international network operators would escalate costs to a degree that few companies would be able to participate. In the most extreme eventuality, it could grind globalization to a halt.

232. *See Cybersecurity Law*, *supra* note 6, art. 7.

233. *See id.* art. 37.

234. *See* Laura DeNardis, *Five Destabilizing Trends in Internet Governance*, 12 I/S: J. L. & Pol'y for Info. Soc'y 113, 128–29 (2015).

235. Winfield & Mendoza, *supra* note 206, at 86 (quoting Jack Goldsmith & Tim Wu, Who Controls the Internet? 104 (2006)).

236. *See* Brown & Yung, *supra* note 1; *see also* Chander & Le, *supra* note 46, at 703–04; *see also* Chang, *supra* note 57, at 15; *see also Digital Divide*, *supra* note 37, at 168–69.

237. *See* Winfield & Mendoza, *supra* note 206, at 92–93 (discussing how China is increasing global suppression by increasing demand for censorship technologies and lobbying for greater international control of Internet resources).

V. CONCLUSION

While the government's reasoning behind the passing of this law is not surprising, and falls in line with Chinese cybersecurity policies that have come before it, this could still place a heavy, or even fatal, burden on businesses trying to cater to the Chinese market. Not only are network operators under threat of their area being considered CI at any point in time, but the results of such a finding would essentially conscript the operator into serving as government censors.[238] What this law makes plainly clear is that protectionist cybersecurity policies have much in common with protective tariffs. While both seek to support local production and enhance security, they actually stifle innovation by weakening competition, and the local population is left in even worse position than before. Ironically, this will most likely harm the Chinese themselves, as their government now peers more deeply into their daily lives and allows for stagnation to grip the market for technology related to cybersecurity.

238. *See Cybersecurity Law*, *supra* note 6, arts. 12, 50, 68–69.