Journal of Strategic Security

Volume 10 | Number 1 Article 2

China's Cyber Initiatives Counter International Pressure

Emilio Iasiello
Private Sector, iasiello@aol.com

pp. 1-16

Recommended Citation
Iasiello, Emilio. "China's Cyber Initiatives Counter International Pressure." *Journal of Strategic Security* 10, no. 1 (2017): : 1-16.
DOI: http://doi.org/10.5038/1944-0472.10.1.1548
Available at: http://scholarcommons.usf.edu/jss/vol10/iss1/2

China’s Cyber Initiatives Counter International Pressure

Author Biography

Emilio Iasiello has more than 12 years' experience as a strategic cyber intelligence analyst, supporting US government civilian and military intelligence organizations, as well as the private sector. He has delivered cyber threat presentations to domestic and international audiences and has published extensively in peer-reviewed journals.

Abstract

Prior to its historic 2015 “no hack” pact for commercial advantage with the United States, Beijing has been engaged drafting and passing legislation, most with specific cyber components, to enhance its security posture while protecting its economic interests. This approach is in stark contrast to United States efforts that have demonstrated a focus on “acting globally, thinking locally” philosophy wherein most of its cyber efforts have been outwardly facing and are distinct from other security considerations. This paper suggests that by strengthening its domestic front with a legal framework, Beijing is preparing itself to counter any foreign initiative contrary to Beijing’s plans (e.g., cyber norms of behavior, cyber sanctions, etc.) by being able to exert legal measures against foreign interests in country, thereby preserving its cyber sovereignty.

Introduction

During the period where the United States threatened to impose cyber sanctions against China for suspected industrial espionage, Beijing has been busy drafting and passing internal legislation to enhance its security posture while protecting its economic interests. Many critics of this series of draft legislation, particular its draft Cybersecurity Law, believe that China is seeking to increase its control over domestic Internet activity and the information traversing it, or using its strict mandates to protect Chinese businesses from foreign competition. One interpretation of the aggressive initiatives undertaken by Beijing is that they reflect an "acting locally, thinking globally" approach to China's security situation, intentionally integrating cybersecurity into all facets of its national strategy. The result is that Beijing is guaranteeing its self-described right of *cyber sovereignty*, a term that remains contested in the international community. Internet security is a national priority due to its interconnected nature with China's informatization strategy, the national-level plan to modernize all facets of China's society. Indeed, the comprehensive nature of China's recently enacted National Security law suggests that Beijing is positioning itself for greater resiliency in the face of exterior influence and pressure in an attempt to mitigate and lessen potential economic and/or diplomatic liabilities imposed by the West.

Definitions

For the purpose of this article, the following definitions are applied.

Cyber sovereignty. In December 2015, Xi Jinping referred a nation's right to choose how to develop and regulate their Internet.[1] In this vein, cyber sovereignty reflects the stance that cyberspace should be defined and ruled by state boundaries.[2]

Cyberspace. The environment formed by physical and nonphysical components, characterized by the use of computers and the electro-magnetic spectrum to store, modify, and exchange data using computer networks.[3]

---

[1] "China Internet: Xi Jinping Calls for Cyber Sovereignty," *BBC News*, December 16, 2015, available at: *http://www.bbc.com/news/world-asia-china-35109453*.
[2] John Costello and Peter Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations," *China's Evolving Military Strategy* (Washington, DC: April 2016).
[3] The Tallinn Manual on the International Law Applicable to Cyber Warfare, March 28, 2013, available at:

Information security. China does not use the word *cyber* and prefers the term information security as it includes the mental aspects of information as well as the technology on which it is processed and shared.[4]

China and Information Security

The fundamental difference between how China and the United States view cyberspace is clear in their respective interpretations on what constitutes cyber security. While the United States maintains a technological view of cyberspace, China is more holistic in its perception taking into account not only the technology that facilitates communications, but also the actual data that traverses or is stored on it.[5] This all-inclusive perception is essential in understanding how China approaches its own security. In February 2014, Chinese President Xi Jinping said that there was no national security without cyber security.[6] The fact that the two have mutual reliance not only highlights China's understanding of the connective nature of networks, but that equally, if not more important, that data and information are the true drivers for creating a secure environment.

Rarely do actors exploit networks for its own sake (although in times of conflict networks may be the targets for disruption or destruction); rather, as the volume of global cyber espionage activity suggests it is the information the network possesses that is valuable, whether it is to a country, a foreign government, or non-state actors. Indeed, China is well aware of the influence potential that information can have, particularly about inciting dissent in a country. China's leaders saw the Color Revolutions as illegitimate actions that removed standing powers, significantly helped by raging domestic grievances, electoral politics exploited by the opposition, and Western powers' intervention for geo-strategic interest.[7] The Chinese government sees its role as a holistic enabler supporting the protection and development of

---

https://issuu.com/nato_ccd_coe/docs/tallinnmanual?layout=http://skin.issuu.com/v/light/layout.xml&showFlipBtn=true&e=5903855/1802381.

[4] Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, English, and Russian," 2013 5th International Conference on Cyber Conflict, available at: *https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf*.

[5] Ibid.

[6] "President Xi Jinping's Views on the Internet," *China Daily*, December 14, 2015, available at: *http://usa.chinadaily.com.cn/china/2015-12/14/content_22706983_3.htm*.

[7] Titus C. Chen, "China's Reaction to the Colored Revolutions: Adaptive Authoritarianism in Full Swing," *National Chengchi University (NCCU)–Institute of International Relations*, 2010, available at: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1644372*.

http://scholarcommons.usf.edu/jss/vol10/iss1/2
DOI: http://doi.org/10.5038/1944-0472.10.1.1548

economic and social initiatives through its series of strategic national Five Year Plans. Due to important part that cyberspace—both the technology as well as the information traversing it—plays in driving economic prosperity and promoting social harmony, it's easy to see why China believes that focusing solely on the infrastructure is too limiting, and does not take into account a country's security and development as well as its people's life and work."[8] Therefore, without willing to make concessions, it comes as little surprise that the two governments have thus far failed to make significant progress in trying to establish norms of behavior in cyberspace, or come to consensus on what constitutes cybersecurity. A mid-September 2015 meeting between Chinese and U.S. officials made headway on this issue, but as of this writing, there remains a fundamental area of disagreement on some important tenets.

Similar to other governments, the issue of cybersecurity has become a major concern for Beijing that has resulted in new agencies being created as well as new legislation being put forth in order to consolidate cybersecurity efforts. This is a vital national imperative for China, a fact evidenced by ever-increasing efforts to control information in country. While trying to increase indigenous production of information technology to reduce reliance on foreign products, China maintains two objectives whose missions ultimately serve the same purpose: preserving the Chinese Communist Party in power.

Key Government Security Initiatives with Cyber Implications

China co-sponsored two proposals for an international code of conduct for nation state use of information and telecommunication technologies–the first presented before the United Nations in 2011, and a revised version in 2015—that have essentially made little headway.[9] In both, China appears to have focused on information security-related initiatives whose outcomes it can control and that directly support China's interests domestically. One of the

[8] William Wan, "Chinese President Xi Jinping Takes Charge of New Cyber Effort," *The Washington Post*, February 27, 2014, available at: *https://www.washingtonpost.com/world/chinese-president-takes-charge-of-new-cyber-effort/2014/02/27/a4bffaac-9fc9-11e3-b8d8-94577ff66b28_story.html*.

[9] Letter dated September 12, 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A//66/359/, September 9, 2011, available at: *https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf;* Letter dated January 9, 2015 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A//69/723/, January 13, 2015, available at: *https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf*.

first key initiatives instituted was the 2014 establishment of a Xi Jinping-led national-level Internet security-leading group to provide critical policy guidance for Internet-related activities in China.

The second initiative is a series of legislation each focusing on areas of national security concerns, each composed of Information security components. Critics view much of this new legislation as China exerting protectionism in order to deter competition while promoting its own companies. However, when viewed through a holistic security prism, the two are not mutually exclusive and if economic development is a Chinese national priority, ensuring that those companies viewed as integral to supporting or driving the country's economic progress is a national security priority, and will likely be supported by government activities. [10] During his September 2015 to the United States, Xi Jinping commented, "We will continue to build a law-based business environment" emphasizing an almost quid-pro-quo relationship. China will continue to open up its marketplace as long as the United States reduces its limits on what American companies can sell in China as well as a "level playing field" for Chinese investment in the United States.[11]

China's recently drafted legislation covers a diverse spectrum of economic and security concerns to include national security, non-governmental organizations, anti-terrorism, and cyber security. However, it is noteworthy that technology and its proper use was a component in much of this legislation, establishing a baseline and providing China a legal means to identify and mitigate any behavior outside what it deems acceptable. Alternatively, it reaffirms China's right to dictate the regulation of its cyberspace and provides China the legal justification to do so. Not only does this reaffirm Xi's acknowledgement that without cybersecurity there is no national security, but with the inclusion of such mandates Beijing is subtly guaranteeing its rights for cyber sovereignty, a term that it first introduced in its 2010 white article, "The Internet in China."[12]

---

[10] Eswar Prasad, "China's Approach to Economic Development and Industrial Policy," *Brookings Institution*, June 15, 2011, available at: *http://www.brookings.edu/research/testimony/2011/06/15-china-economic-development-prasad*.

[11] Todd C. Frankel, "China's President Promises to Open Doors to U.S. Businesses," *The Washington Post*, September 23, 2015, available at: *https://www.washingtonpost.com/business/economy/china-president-pledges-to-open-doors-to-us-businesses/2015/09/23/298d24e0-94d6-4064-930a-b21578916b8d_story.html*.

[12] Shannon Tiezzi, "China's Sovereign Internet," *The Diplomat*, June 24, 2014, available at: *http://thediplomat.com/2014/06/chinas-sovereign-internet/*.

http://scholarcommons.usf.edu/jss/vol10/iss1/2
DOI: http://doi.org/10.5038/1944-0472.10.1.1548

Creation of the Central Internet Security and Informatization Leading Group

While the Chinese government bureaucratic hierarchy resembles that of other governments, leading small groups composed of senior influential officials drive important policy decisions. Leading groups, which rarely announce their meetings or disclose their full membership, cover everything from economics to propaganda working out policy decisions long before the party receives them.[13] According to the director of a Chinese policy institute, small groups rather than government ministries decide important policy matters.[14]

In February 2014, Chinese President Xi Jinping assumed charge of a new Central Committee leading group overseeing Chinese Internet security, the Central Internet Security and Informatization Leading Group. State-run CCTV outlined several goals of the group, including the drafting of a comprehensive national cybersecurity strategy and coordination of cybersecurity across sectors. According to CCTV, Xi tied the importance of government work on securing the Internet to long-term priorities, such as maintaining control over public opinion in China.[15]

Additionally, according to Chinese news sources, this leading group is to deepen reform, protect national security, safeguard national interests, and promote the development of information technology. The group will have complete authority over online activities, including economic, political, cultural, social, and military. [16] The leading group's close relationship to China's State Council, the chief administrative authority of the country, enables rapid implementation of guidelines and laws.[17]

---

[13] Cary Huang, "How Leading Small Groups Help Xi Jinping and other Party Leaders Exert Power," *South China Morning Post,* September 14, 2014, available at: *http://www.scmp.com/news/china/article/1409118/how-leading-small-groups-help-xi-jinping-and-other-party-leaders-exert*.
[14] Ibid.
[15] William Wan, "Chinese President Xi Jinping Takes Charge of New Cyber Effort," *The Washington Post*, February 27, 2014, available at: *https://www.washingtonpost.com/world/chinese-president-takes-charge-of-new-cyber-effort/2014/02/27/a4bffaac-9fc9-11e3-b8d8-94577ff66b28_story.html*.
[16] "Central Leading Group for Internet Security and Informatization Established," China Copyright and Media, March 13, 2014, available at: *https://chinacopyrightandmedia.wordpress.com/2014/03/01/central-leading-group-for-internet-security-and-informatization-established/*.
[17] "China Monitor," *Mercator Institute for China Studies*, December 2014, available at: *http://www.merics.org/fileadmin/user_upload/downloads/China-Monitor/China_Monitor_No_20_eng.pdf*.

The leading group's membership demonstrates China's commitment in raising cybersecurity to the national level, providing a decision-making authority. The senior-level membership to include the President and the Premier reflect Beijing's direct involvement in the creation and implementation of future cyber policy for the country. Indeed, China designed its "Outline of National IT Development Strategy" to guide the country's IT development for the next decade and position China to become an Internet power by 2050.[18]

Passing the 2016 "Cyber Security" Law

In November 2016, the Chinese government approved its "Cyber Security" Law, which addresses the security of key Internet and information systems and data,[19] as well as increasing the government's powers to record and impede the dissemination of information it deemed illegal.[20] Introduced by the Cybersecurity Administration of China (CAC), an organization created in 2014 to consolidate control over cybersecurity, the law is set to go into effect in June 2017.[21] Per the law, government agencies would issue additional guidelines for network security in "critical industries" such as telecoms, energy, transport, finance, national defense and military matters, and government administration, according to a news source.[22] Agencies and enterprises will be compelled to improve their ability to defend against network intrusions while demanding security reviews for equipment and data.[23] The government will adopt priority protection over key information infrastructure that seriously jeopardizes national security and the public

---

[18] "China Eyes World Class Cyber Multi-Nationals," *Xinhua*, July 27, 2016, available at: *http://news.xinhuanet.com/english/2016-07/27/c_135544563.htm;* Mandy Zuo, "China Aims to Become Internet Superpower by 2050," *South China Morning Post*, July 28, 2016, available at: *http://www.scmp.com/news/china/policies-politics/article/1995936/china-aims-become-internet-cyberpower-2020*.
[19] "China Passes New National Security Law Extending Control over the Internet," *The Guardian*, July 1, 2015, available at: *http://www.theguardian.com/world/2015/jul/01/china-national-security-law-internet-regulation-cyberspace-xi-jinping*.
[20] Gerry Shih, "China Draft Cyber Security Law Could up Censorship, Irk Business," *Reuters*, July 8, 2015, available at: *http://www.reuters.com/article/2015/07/08/us-china-cybersecurity-idUSKCN0PI09020150708*.
[21] Josh Chin and Eva Dou, "China's New Cybersecurity Law Rattles Foreign Tech Firms," *Wall Street Journal*, November 7, 2016 available at: *http://www.wsj.com/articles/china-approves-cybersecurity-law-1478491064*.
[22] Gerry Shih, "China Draft Cyber Security Law Could up Censorship, Irk Business," *Reuters*, July 8, 2015, available at: *http://www.reuters.com/article/2015/07/08/us-china-cybersecurity-idUSKCN0PI09020150708*.
[23] Chin and Dou, "China's New Cybersecurity Law."

http://scholarcommons.usf.edu/jss/vol10/iss1/2
DOI: http://doi.org/10.5038/1944-0472.10.1.1548

interest, particularly in the event of damaged or leaked data.[24] According to one Chinese media outlet, the law safeguards sovereignty on cyberspace, national security, and the rights of citizens.[25]

Internationally, the law faces much trepidation. Critics believe that such a bill would further protect China products, conveying that such legislation could make it difficult for countries that rely on competition to bolster their economic interests.[26] Other critics cite the provisions of making censorship a matter of cybersecurity, which ultimately would allow the government to punish those companies that allow unapproved online publication of information online.[27] Certainly, the fact that the law requires information produced in China to remain in China can make it difficult for foreign vendors, particularly of tech equipment, considering that all network equipment must meet Chinese government approval prior to deployment.[28] However, some see the law as bolstering the security of the domestic population. As one source points out, most of the privacy enhancements benefiting Chinese citizens (to include access, data retention, breach notification, mobile privacy, online fraud, and protection of minors) align with those required in the European Union.[29]

The urgency of this law reflects Beijing's prioritization of the use of the Internet particularly as it applies to its national security, which may be the reason why many of the same issues feature prominently in both the national security law and the new cybersecurity law. There are two key reoccurring themes: 1) the ability to monitor and control information, and 2) the compliance of foreign enterprises with the rules set forth. Both have been cited by critics as being efforts of the government to tighten its control on civil

---

[24] "Second Reading of China's Draft of Cybersecurity Law," *Lexology*, June 30, 2016, available at: *http://www.lexology.com/library/detail.aspx?g=eaac6bbd-12ab-4459-96cd-ba42a2cee007*.
[25] "Xinhua Insight: China adopts cybersecurity law to protect national security, citizens' rights," *Xinhua.net,* November 7, 2016, available at: *http://news.xinhuanet.com/english/2016-11/07/c_135812209.htm*.
[26] Katie Nelson, "China's Cybersecurity Law–Trouble for Businesses," *The Washington Examiner*, September 8, 2015, available at: *http://www.washingtonexaminer.com/chinas-cybersecurity-law-trouble-for-businesses/article/2571314*.
[27] Chin and Dou, "China's New Cybersecurity Law."
[28] Jonathan Vanian, "How China's Proposed Cybersecurity Law Could Impact Tech Companies," *Fortune*, July 8, 2015, available at: *http://fortune.com/2015/07/08/chinas-proposed-cybersecurity-law-impact-tech-companies/*.
[29] Patrick Burke, "China: Carpe Datum Law Blog China Finalizes Cyber Security Law," *Mondaq,* December 8, 2016, available at: *http://www.mondaq.com/china/x/551194/Security/Carpe+Datum+Law+Blog+China+Finalizes+New+Cyber+Security+Law*.

society while making unreasonable demands on foreign businesses,[30] particularly as it empowers the government to oversee the hardware and software holding the data of foreign companies, as well as look inside at the data.[31] On December 27, CAC published a strategy document that laid out the framework for the new cybersecurity law in which it reiterated the need for increased scrutiny of local and foreign technology used in industries deemed critical to the national interest.[32] While such a mandate may appear draconian, it does align China's strategic security interests with most other nation states, particularly concerning security critical infrastructure.

However, perhaps creating the most uneasiness is the vagueness surrounding the language of the law and the details surrounding how the government intends to monitor compliance, leaving such interpretation up to the authorities in charge. Such broad considerations enable China to implement a case-by-case approach, allowing it to scrutinize the business practices of the companies, as well as any perceived or real government association, to influence and inform decision-making. In such instances, such legal ambiguity provides China the means to implement penalties as a warning or a retaliatory action to perceived threats against Chinese economic and/or political interests.

Passing the 2016 Overseas Non-Government Organization Management Law

The law is designed to standardize foreign non-governmental office (NGO) operations in order to promote "exchange and cooperation" while outlining permissible and non-permissible activities.[33] All NGOs would be required to get approval from a Chinese supervisory unit before it can operate in China, banning those that do not receive such authorization.[34] It further prohibits any Chinese organization from conducting activities on behalf of or with non-

[30] Bethany Allen-Ebrahimian, "The Chilling Effect of China's New Cybersecurity Regime, *Foreign Policy*, July 10, 2015, available at: *http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/*.
[31] Burke, "China: Carpe Datum Law."
[32] Cate Cadell, "China Renews Calls for Tighter Cyber Space Security – CAC," *Reuters*, December 27, 2016, available at: *http://news.trust.org/item/20161227071926-di2or/*.
[33] Jared Genser and Julia Kuperminc, "China's Proposed Non-Governmental Organization Law: Cooperation or Coercion?" *The Diplomat*, July 2, 2015, available at: *http://thediplomat.com/2015/07/chinas-proposed-non-governmental-organization-law-cooperation-or-coercion/*.
[34] Edward Wong, "Clampdown in China Restricts 7,000 Foreign Organizations," *The New York Times*, April 28, 2016, available at: *http://www.nytimes.com/2016/04/29/world/asia/china-foreign-ngo-law.html*.

http://scholarcommons.usf.edu/jss/vol10/iss1/2
DOI: http://doi.org/10.5038/1944-0472.10.1.1548

authorized NGOs.[35] Critics are pressing Beijing to revise the current draft due to concerns that the law would greatly influence Chinese civil society, restricting freedoms, and tightening control of expression within China.[36] Like the National Security and draft Cybersecurity law, the NGO law is nebulous concerning definitions affording Beijing considerable grey area in which to operate. For example, identifying criteria for what constitutes an NGO is unclear and possibly ranges from a foreign professor visiting China to an artistic dance troupe.[37] Additionally worrisome is that the law forbids *political activities* without clarifying activity classification or providing the evaluation criteria informing this determination.[38] While the law is not specifically cyber-related, it is safe to assume that NGOs that properly register with Chinese authorities would be required to comply with any acceptable technology use policies set forth by the Chinese government in other legislation.

Passing the 2015 National Security Law

On July 1, 2015, China's Standing Committee of the National People's Congress adopted a new National Security Law, largely considered China's most comprehensive national security legislation. According to one U.S. law firm specializing in international national security matters, the main function of the law is to provide a framework for China's security considerations in the face of emerging threats; however, overlapping security considerations in many areas demonstrate Beijing's perspective that national security is an inherently integrated process, creating "a national security path with Chinese characteristics."[39] The law breaks down into the following seven chapters:

- Guiding principles for national security
- Defining national security across multiple areas (e.g., cultural, economic, and military security)

---

[35] "China: The Draft Overseas NGO Management Law Must be Substantially Revised," *FIDH*, June 3, 2015, available at: *https://www.fidh.org/International-Federation-for-Human-Rights/asia/china/china-the-draft-overseas-ngo-management-law-must-be-substantially*.
[36] Sui-Lee Wee, Michael Martina, and James Pomfret, "Foreign Governments, Non-Profits Press China to Revise NGO Law," *Reuters*, June 1, 2015, available at: *http://www.reuters.com/article/2015/06/01/us-china-ngos-idUSKBN0OH2I720150601*.
[37] Ibid.
[38] Genser and Kuperminc, "China's Proposed Non-Governmental Organization Law."
[39] Zunou Zhou, "China's Draft Counter-Terrorism Law," *Jamestown Foundation*, July 17, 2015, available at: *http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews[tt_news]=44173&cHash=dc00eedd4c61b21c691b9700b1468049#.VfwKd3szAZQ*.

- Functions and responsibilities of the National People's Congress
- Key elements of the national security regime (e.g., intelligence collection, states of emergency)
- Allocating resources to national security work
- Obligations of citizens and corporations to national security
- Supplementary provisions[40]

Perhaps most notably, however, is that the law is not restrictive to China's borders. Included in China's territorial sovereignty includes the polar beds, outer space, and cyberspace, a much wider aperture than narrower perspectives on national security that focus more on defense.[41] This should come as little surprise given Beijing's continued advocacy for a state's right of territorial sovereignty, particularly in areas such as cyberspace and outer space. With cyberspace, China views information as well as information systems in the same context, intimating that information even outside China's borders is a potential threat to its national security interests. [42]

Critics of the new law cite two major concerns about the legislation's wording and implication. The first is that the law is widely seen as Beijing's commitment to increasing its monitoring and control of internal dissent, while government officials view it as a necessary tool to address new and emerging threats such as cybercrime and terrorism.[43] Many believe that China cracks down on opposition, a capability greatly enhanced by the broad powers imparted to authorities under the current wording of the new law. One major criticism is that the stated provisions are vague, lacking the necessary details to provide a more concrete understanding of what is acceptable and where the line is drawn and what are acceptable repercussions. Such ambiguity appears left up to the discretion and interpretation of authorities providing them a wide berth from which to operate.

---

[40] "China Enacts New National Security Law," *Covington*, July 2, 2015, available at: *https://www.cov.com/~/media/files/corporate/publications/2015/06/china_passes_new_national_security_law.pdf*.
[41] "China's New National Security Law Creates More Insecurity for Foreign Businesses," *Hogan Lovells*, July 2015, available at: *https://www.hoganlovells.com/en/publications/chinas-new-national-security-law-creates-more-insecurity-for-foreign-businesses*.
[42] Bethany Allen-Ebrahimian, "The Chilling Effect of China's New Cybersecurity Regime, *Foreign Policy*, July 10, 2015, available at: *http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/*.
[43] Chun Han Wong, "China Adopts Sweeping National-Security Law," *The Wall Street Journal*, July 1, 2015, available at: *http://www.wsj.com/articles/china-adopts-sweeping-national-security-law-1435757589*.

http://scholarcommons.usf.edu/jss/vol10/iss1/2
DOI: http://doi.org/10.5038/1944-0472.10.1.1548

The second concern is that the law's focus on foreign technology products and services is a move to promote Chinese companies over foreign competitors. Core network technology, critical infrastructure, and information systems and data in key areas are to be stored securely and be controllable.[44] Unsurprisingly, this is garnering much concern from foreign companies that would fall under these requirements under Article 59, which focuses on national security review and monitoring "foreign investment that infringes upon or may infringe upon national security."[45] This may result in serious implications for foreign suppliers of such equipment and/or services, such as the imposition of higher costs or scrutiny than their Chinese counterparts.

If the national security law is the foundation from which its subsequent draft legislation has emerged, China's May 2015 Military Strategy is the underpinning for many of these sovereignty themes. The strategy emphasizes China's national security situation against a world of complex threats, taking the opportunity to address specifically space and cyberspace as the new commanding heights in strategic competition.[46] Indeed, China's national level policy reinforces messaging that addresses China's peaceful rise in a time of increasing and diverse threats making integrated security planning an essential counterweight.

Passing the 2015 Anti-Terror Law

In December 2015, China passed a new "anti-terror law" that compels technology companies to help decrypt information giving Chinese authorities access to encrypted data.[47] The law combined administrative, judicial, and military means to address Chinese anti-terrorism efforts, demonstrating a comprehensiveness that reflects Beijing's desire to integrate all facets of security under the umbrella of its new national security law. The law reinforces tenets seen in the other draft legislation: aspects of information control, organizational monitoring, technology compliance, and collaboration with Chinese authorities in the name of security. For example, the proposed

---

[44] "China's New National Security Law Creates More Insecurity."
[45] "China Enacts New National Security Law."
[46] Caitlin Campbell, "Highlights from China's New Defense White Paper, 'China's Military Strategy," *U.S.-China Economic and Security Review Commission*, June 1, 2015 available at: *http://origin.www.uscc.gov/sites/default/files/Research/Issue%20Brief_Highlights%20from%20Chinas%20New%20Defense%20White%20Paper_Campbell_6.1.15.pdf*.
[47] "China Passes Anti-Terror Law with Controversial Cyber Provisions," *Reuters*, December 28, 2015, available at: *http://www.nbcnews.com/tech/tech-news/china-passes-anti-terror-law-controversial-cyber-provisions-n486756*.

law would also require companies to keep also servers and user data within China, supply law enforcement authorities with communications records and censor terrorism-related Internet content.[48] In the face of mounting pressure, China ultimately amended some of the initial provisions that would have mandated technology companies to provide backdoor access for Chinese authorities' remote access. Ultimately, the final enacted law did not include these provisions.[49]

Developing and Using IT Standards

While China pushes forward its legislative agenda, it also approaches its security from technological perspective where it continually seeks ways to reduce dependence on foreign technologies. One approach toward this end is the development of alternative standards to help boost their own companies. National Security Agency (NSA) whistleblower Edward Snowden's disclosures of alleged collusion between U.S. technology firms and the NSA only magnified China's fears of foreign technology resulting in China removing some U.S. companies from government-approved purchase lists.[50] The following are some initiatives that China has embarked upon to reach this objective.

- China's Multi-Level Protection Scheme (MLPS): First introduced in 2007, China's MLPS protects Chinese national security, although detractors believe it also serves to protect Chinese industry from international competition.[51] The MLPS has a five-level risk-based classification to identify and protect those systems that are critical for national security and the economy (Level 3 and above).[52] In concert

[48] Michael Martina, "China Says Deliberation on Draft Anti-Terrorism Law Goes Ahead," *Reuters*, March 17, 2015, available at: *http://www.reuters.com/article/2015/03/17/us-china-security-idUSKBN0MD12X20150317*.
[49] Glyn Moody, "China's New Anti-Terror Law: No Backdoors, but Decryption on Demand," *Ars Technica*, December 29, 2015, available at: *http://arstechnica.com/tech-policy/2015/12/chinas-new-anti-terror-law-copies-uk-no-backdoors-but-decryption-on-demand/*.
[50] Scott Cendrowski, "Why China Is Making Life Miserable for Big U.S. Tech," *Forbes*, February 26, 2015, available at: *http://fortune.com/2015/02/26/why-china-is-making-life-miserable-for-big-u-s-tech/*.
[51] Nathaniel Ahrens, "National Security and China's Information Security Standards," *Center for Strategic & International Studies*, November 8, 2012, available at: *http://csis.org/publication/national-security-and-chinas-information-security-standards*.
[52] Jing de Jong-Chen, "U.S.-China Cybersecurity Relations: Understanding China's Current Environment," *Georgetown Journal of International Affairs*, September 15, 2014, available at: *http://journal.georgetown.edu/u-s-china-cybersecurity-relations-understanding-chinas-current-environment/*.

http://scholarcommons.usf.edu/jss/vol10/iss1/2
DOI: http://doi.org/10.5038/1944-0472.10.1.1548

with the MLPS strategy, China has ventured forth in trying to develop alternative standards to compete with Western-led standardization efforts. Some of these include:

- *WAPI*: China was working to adopt Wireless LAN Authentication and Privacy Infrastructure (WAPI) as a mandatory security measure for any wireless product sold in China. However, after objections from the U.S. government and other IT companies, it suspended efforts in 2014.[53]

- *Payments Standard*: Additionally, in June 2015, China implemented a payments standard requiring all bank cards issued in China to comply with a technical standard known as PBOC 3.0. The new standard would force companies like MasterCard and Visa to adopt the new standard at a significant cost. While cited as a security concern, detractors assert that China is using this standard as an "unnecessary barrier to trade."[54]

Legal Warfare–Prepping for Future Conflict

Viewed through the prism of *legal warfare*, the onslaught of draft legislation bolsters China's strategy to exploit domestic and international laws in order to achieve the legal high ground or assert Chinese interests.[55] At its core, before the onset of actual formal hostilities and continuing after their conclusion, the strategic goal of legal warfare provides pre-conflict justification and post-conflict legal resolution.[56]

Passed legislation focuses on areas that not only improve Chinese security, but also provide the legal justification for Chinese authorities to act in any manner they determine is appropriate. The ambiguity inherent in each draft

---

[53] Grant Gross, "China Agrees to Drop WAPI Standard," *Computer World*, April 22, 2004, available at: *http://www.computerworld.com/article/2565021/mobile-wireless/china-agrees-to-drop-wapi-standard.html*.
[54] Gabriel Wildau, "Visa and MasterCard Face Down China Techno-Nationalism," *Financial Times*, June 14, 2015, available at: *https://app.ft.com/cms/s/f3ac0dfa-05d9-11e5-868c-00144feabdc0.html*.
[55] "China: The Three Warfares," Prepared for the Office of the Secretary of Defense, May 2013, available at: *https://cryptome.org/2014/06/prc-three-wars.pdf*.
[56] Dean Cheng, "Winning Without Fighting: Chinese Legal Warfare," *Heritage Foundation*, May 21, 2012, available at: *http://www.heritage.org/research/reports/2012/05/winning-without-fighting-chinese-legal-warfare*.

bill allows operational freedom for the government allowing it to determine criminal acts and corresponding consequences to their offenses.

When viewing requirements placed on foreign interests in China, failure to comply provides the government a legal avenue to pursue repercussions. The legal nebulousness provides China the wiggle room to pursue other means of resolution to safeguard its interests in other political, diplomatic, or economic areas. For example, should the United States ultimately levy cyber sanctions against China for their espionage activities, China is able to look at U.S. companies in China and find the legal means with which to impose fines or expel them from business from China as a retaliatory action that is backed by the legal grounds the government has established. The fact that businesses have to agree to these rules in order to do business in China means that they acknowledged and understood the laws previously giving them little recourse to appealing the matter.

Acting Locally–What Does It Mean for China?

By acting locally about implementing cybersecurity in all of its legislation, China is legally guaranteeing its rights as a cyber sovereign, thereby providing the justification to mitigate direct threats to its national security via the information space. The fact that Beijing views its national security as a closely interwoven tapestry of concerns with information security as its unifying thread suggests that it will continue to view "cyber" security from a holistic perspective, and not just a technical one and not just a technical one disconnected from the data it protects. Overlapping rules ultimately offer the government plenty of opportunities to target individuals/organizations under various statutes, thereby providing it a diverse and flexible platform from which to respond to any perceived hostile infractions to China's information space. They also offer Beijing a retaliatory mechanism for incurred penalties like cyber sanctions that levied against Chinese interests.

Termed "protectionist" by critics, these legislative initiatives accomplish the goal of strengthening China's strategic security interests (which include regime power continuity, sustaining economic growth, domestic stability, defending national and territorial sovereignty, and reacquiring regional preeminence).[57] Therefore, when governments admonish Beijing for

[57] "Military and Security Developments Involving the People's Republic of China 2015," *Office of the Secretary of Defense*, available at: *http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf*.

http://scholarcommons.usf.edu/jss/vol10/iss1/2
DOI: http://doi.org/10.5038/1944-0472.10.1.1548

supporting its commercial sector via government requirements that restrain foreign businesses in country, Beijing can leverage these laws to support these same national security interests. The same principle extends to conducting cyber espionage for intellectual property for that matter, as long as it does not conflict with the principles set forth in the 2015 China-U.S. "no hacking for commercial gain" agreement.

"Acting locally" via recent legislation enables China to address better its strategic security objectives by positioning China to be able to mitigate potential fallout from those situations that could negatively affect China's interests. Some of these include but are not limited to the following:

- A Chinese Color Revolution: Beijing is acutely aware of the successes the various Color Revolutions had on regime change in their respective countries. Beijing has survived similar scares in the past: The 1989 Tiananmen Square student-led protests called for press and speech freedoms. The protests culminated in a million people gathering at its height and required military intervention to quell it.[58] In 2014, authorities ultimately put down Hong Kong's pro-democratic "Occupy Central" protesters after two months of protesting.[59] Monitoring and controlling information venues, as well as any NGO in country, certainly mitigates the opportunities for harmful information to work its way into the public domain.

- Non-China Friendly Cyber Norms of Behavior: While there is not a currently an accepted international cyber, code of conduct, both the United States and China and Russia have been promoting their own visions of what such an agreement should encompass. Should the global consensus favor the model advocated by the United States and Western interests, Beijing can enforce the standards set forth by this series of legislation as they dictate the rule of conduct for organizations in its sovereign territory.

Conclusion

[58] William Wan and Simon Denyer, "In Tiananmen Square No Trace of Remembrance on 25th Anniversary," *The Washington Post*, June 4, 2014, available at: *https://www.washingtonpost.com/world/security-tight-as-china-represses-tiananmen-anniversary/2014/06/04/4d1c39e9-84c4-475c-a07a-03f1d2dd9cdf_story.html*.
[59] "Hong Kong Protests: What Changed at Mong Kok?" *BBC News*, December 3, 2014, available at: *http://www.bbc.com/news/world-asia-china-29054196*.

China's new legislation comes at a time when Beijing is actively seeking to improve its security posture, while concurrently trying to preserve its vital interests, particularly an economy which had experienced substantial growth but has since slowed down considerably in 2015.[60] The series of draft legislation focuses internally and in several cases contain overlapping regulations designed to enforce the same rules. Vague language and lack of clear criteria will ultimately benefit the Chinese who will be able to use their own judgment in reviewing potential infractions on a case-by-case basis, allowing them to levy punishment per their assignment of value (and perhaps influenced by geopolitical matters).

China's belief that information security integrates with other security disciplines demonstrates its commitment to addressing its acknowledged weaknesses in the digital domain. The establishment of a national-level leading group whose mission is to protect national security, safeguard national interests, and promote the development of information technology, underscores this undertaking.[61] The close relationship with the leading group and the State Council further shows that such collaboration better ensures the rapid implementation of guidelines and laws.[62] The onslaught of draft legislation and the prompt enactment of its new National Security Law are indicative of the success of this collaboration.

It is too early to tell if China will push the seemingly restrictive parameters of their recent legislation drafts, are temper them more in order to assuage foreign concerns. The result of Xi's 2015 state visit and political/economic responses to alleged Chinese cyber activity, as well as other geopolitical hotspots such as South China Sea disputes will likely influence the ultimate verbiage, passage, and enforcement of these laws. Based on previous history, Beijing will likely wait, watch, and act accordingly.

---

[60] "China's Economic Challenges Persist," Voice of America, September 14, 2015, available at: *http://www.voanews.com/content/chinas-economic-challenges-persist/2962833.html*.
[61] "Central Leading Group for Internet Security and Informatization Established," *China Copyright and Media*, March 11, 2014, available at: *https://chinacopyrightandmedia.wordpress.com/2014/03/01/central-leading-group-for-internet-security-and-informatization-established/*.
[62] "China Monitor," *Mercator Institute for China Studies*, December 2014, available at: *http://www.merics.org/fileadmin/user_upload/downloads/China-Monitor/China_Monitor_No_20_eng.pdf*.

http://scholarcommons.usf.edu/jss/vol10/iss1/2
DOI: http://doi.org/10.5038/1944-0472.10.1.1548