National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# THE IMPLICATIONS OF CYBER ON US-CHINA RELATIONS

Maj J. Johnson

## JCSP 43

## Exercise *Solo Flight*

**Disclaimer**

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.



## PCEMI 43

## Exercice *Solo Flight*

**Avertissement**

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.



Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 – PCEMI 43
2016 – 2017

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

# THE IMPLICATIONS OF CYBER ON US-CHINA RELATIONS

Maj J. Johnson



Word Count: 5492

Compte de mots: 5492

## Introduction

Cyber seems to dominate the US-China relations, which has emerged as one of the most complex and vital forces with immeasurable impact on the world stage, given the economic prowess of the two nations. The relationship is characterized by deep mistrust and conflict due to competing geopolitical interests, historical differences, and ideological constraints. Recently, the tension has increased significantly due to a number of cyber incidents linked to the Chinese government that targeted American economic and national security interests. China's rising power has been unsettling given its aggressive modernization of the People's Liberation Army (PLA) in space, cyberspace, and certain conventional military capabilities such as ballistic missile and Intelligence, Surveillance and Reconnaissance technology that supports an asymmetric posture against the powerful United States military.

Despite the growing concerns of its neighbor, China's assertive approach in the South China Sea seems to betray its narrative regarding a peaceful rise. The US presence in the region provides assurance to allies and sends an explicit message to Beijing about the need to respect international norms. This backdrop along with historical differences and increasing malicious cyber intrusions obfuscate China's intent, creating a security dilemma, which extends to the cyber domain. Given China's propensity to link economic development to security and political survival, its recent deteriorating economic situation arguably provided an avenue of approach to hold open and honest discussions about cyber. In 2015, the US threatened significant economic pressure to address the cyber security tensions, which compelled the Chinese to sign a Cyber Security Agreement with emphasis on containing malicious cyber activities that affect the economic landscape. Given the chasm between the two nations, question remains as to whether the differences

are reconcilable despite the agreement. So, how substantive and enforceable is the agreement? Upon further scrutiny, it merely represents open dialogue to relieve the pressure, affording China space to recalibrate its cyber strategy to enhance the sophistication of the cyber intrusions while significantly reducing detection.

The deleterious impact of a potential cyber-induced conflict requires a cooperative framework to manage the complexity and unpredictability of US-China relations in cyber security. A comprehensive understanding of the risks, common ground, and areas of disagreement is vital for solidifying cooperation between the two most powerful players in the cyber sphere. Nationalistic tendencies tend to complicate matters and must be suppressed with pragmatism to avoid unnecessary escalation based on ideological fervor.

The characteristics of cyber such as difficulty of attribution, diverse terminology, offensive advantage to maximize power in that sphere, decentralization, low barriers to entry and innovation outpacing policy catapults cyberspace as a tenuous affair that demands a meticulous structure to avert miscalculation and overreaction that can easily spillover on the diplomatic, military, and economic dimensions of international relations. The framework must recognize the Chinese right to conduct military espionage while establishing norms that both countries can endorse on the international stage through existing organizational structures. This paper peruses the Cyber Security Agreement and advances cooperation by exploring the dynamics of US-China relations in the cyber domain and the impact on the international relations landscape. Finally, it proposes an enforceable cooperative framework that builds on the existing agreement.

**US-China Cybersecurity Agreement**

The 2015 US-China Cybersecurity Agreement represents an initial step, but is not effective in and of itself in terms of achieving cooperation in cyberspace and the cessation of economic espionage. The agreement will be analyzed using a three-prong approach: first, explore the conflicting views of national security interests in the cyber sphere; second, contrast China's and US' approach to cyberspace in terms of information control versus network security; Finally, evaluate the agreement to determine its measurable effectiveness. Nigel Inkster from International Institute of Strategic Studies stated, "Since the turn of the 21st century, there has been a massive growth in cyber-exploitation activities operations emanating from China."[1] He indicated China's target centers on government, major corporations, and opponent of the Chinese government.

First, the line between national security interests and economic espionage can be blurred, which has triggered fierce resistance and apathy when the US called China on the carpet due to increasing cyber intrusions. China has accused the US of hypocrisy and militarizing cyber, especially after Snowden indicated the multiple and repeated cyber intrusions into other countries' cyberspace, including allies. The US draws a clear distinction between industry and government, while China regards industry as indispensable to economic security and political survival. Chinese President, Xi Jinping, asserted, "Security and economic development are inextricably linked."[2] China's five-year plan focuses on developing a prosperous China, including enhancing the monitoring[1] and censorship technologies to promote a hygienic modern system by

[1] Nigel Inkster, "China's Cyber Power." (Bell & Bain Ltd: Glasgow), 2016.
[2] Brookings Institution, "China's Security and Foreign Policies: Comparing American and Japanese Perspectives." Last accessed on 30 October 2016, https://www.youtube.com/watch?v=f2Nh-tu2FUI

2020. China has adeptly used its integration into the global market, and the use of patriotic Chinese education and historical narratives to consolidate its grip on power and ensure regime survival.

The Chinese government views legitimacy as a critical factor and seems to frame all of its endeavors in terms of nationalism while restricting the flow information and blunting dissent through coercive means to ensure political stability. For instance, China has galvanized the domestic population with a patriotic narrative by framing the dispute in the South China Sea and East China Sea in terms of sovereignty and territorial integrity.[4] That legitimacy extends to the cyber realm, as China pushes for cyber sovereignty to prevent other countries from interfering with its internal affairs. The proposal seems pointed at the US, as China views freedom of expression, human rights, and open and reliable internet as a threat to its national security and political survival.

China seems to rely heavily on social and economic development for parity with the world's largest economy, the US. Foreign affairs experts from Center of Strategic and International Studies (CSIS) and Peterson Institute for International Economics identified three criteria for a country to be considered an economic superpower: large enough to affect the world economy, dynamic enough to contribute to global growth, and open to trade and capital flows.[5] The Chinese ambassador to the World Trade Organization said during negotiations to join, "We know we have to play the game now but in ten years we will set the rules!"[6] China is now the second largest economic superpower and while its

---

[3] Huaxia, China's Five Year Plan to Benefit the World. Xinhua, 3 Nov 2015. Last accessed on 14 Apr 2017. http://news.xinhuanet.com/english/2015-11/03/c_134780397.htm

[4] Robert G. Sutter, Foreign Relations of the PRC (Maryland: Rowman and Littlefield, 2013), 2.

[5] Fred Bergsten, Charles Freeman, Nicholas Lardy, Derek Mitchell, China's Rise: Threats, Challenges, and Opportunities. (CSIS: Washington D.C.), 2008.

[6] Ibid., 9.

economy has contracted, its trajectory is encouraging as the government engages in significant reforms to modernize its economic structure. China recognizes it faces significant domestic and environmental challenges that may derail its growth and political stability, spurring the constant focus on sanitizing information through propaganda, cyber, and other means while calibrating the agenda for social and economic development.

China's claim in the South China Sea seems to be based on economic development, which may partly explain China's intransigence despite protests from neighbouring countries. The World Bank estimates, "South China Sea holds proven oil reserves of at least 7 billion barrels of oil and 900 trillion cubic feet of natural gas, which offer tremendous economic opportunity…"[7] China's appetite for energy has grown tremendously over the past few decades and is unlikely to subside as the trajectory for economic growth remains solid, albeit slower. Experts from CSIS contend, "…The changes in the structure of the economy (China) pushed energy demand up by 11 percent a year. Today China's share of the global energy use has swelled to over 16 percent, forcing the country to rely on international markets."[8] The US has been at odds with China on this issue and consistently conducts freedom of navigation military operations to preserve international order and as a form of assurance to its allies. China interprets the US actions as interference in domestic affairs and an attempt to contain China's rise. This[2] interpretation affects the cyber arena as well, as China is suspicious of the US dominance in that sphere and seems intent on challenging the US hegemony in the region

---

[7] Beina Xu, South China Sea Tensions. Council on Foreign Relations, 14 May 2014. Last accessed on 15 Apr 2017. http://www.cfr.org/china/south-china-sea-tensions/p29790.

[8] Fred Bergsten, Charles Freeman, Nicholas Lardy, Derek Mitchell, China's Rise: Threats, Challenges, and Opportunities. (CSIS: Washington D.C.), 2008.

through significant investments in its military, space, cyberspace, and economy. The Chinese military PLA Daily stated, "Internet warfare is of equal significance to land, sea, and airpower, and requires its own military branch." [9] China seems impressed with US cyber offensive capabilities and views the necessity for developing offensive technologies that provide effective countermeasures and effective strikes capable of crippling a powerful adversary. The aforementioned factors couple with the history of the rise of the Chinese Communist Party in power are responsible for the coupling of national security with economic development and political stability. Therefore, China being on board with an agreement that focuses on economic espionage seems ingenuine and contradictory with its fundamental belief and values, making verifiable compliance unlikely.

Espionage is a normal activity from virtually every country; however, the alarming rate of Chinese cyber espionage targeting corporate and government networks has strained relations and reinforced the suspicion that China is willing to use duplicitous measures to grow its economic and military power, thereby increasing its global influence at the expense of the US and the West. According to Gary Brown and Christopher Yung from the Diplomat, "The United States has been particularly troubled with China engaging in espionage to benefit their domestic companies and state-owned enterprises."[10] [3]

---

[9] Reveron, Derek S. "Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World." (Georgetown University Press: Washington D.C.), 2012.

[10] Gary Brown and Christopher Yung, How Washington Approaches Cyberspace and its 2015. Cybersecurity Agreement with China. The Diplomat, 19 Jan 2017. Last accessed on 15 Apr 2017. http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/.

The significant trade deficit between US and China provides further suspicion that China is positioning itself through cyber espionage to surpass the US economy. US exports to China are estimated at $55.8 billion while China's export to US at 229.2 billion.[11] China's indigenous policy where foreign companies are expected to disclose their trade secrets in exchange for market access deepened the chasm. This strategy reportedly benefits the domestic companies who develop products based on the secrets and squeeze out the foreign firms. In addition, Chinese hackers become familiar with the technology and leverage that knowledge to deploy effective hacking methodologies against the US, western companies, and government. While the bulk of the exports represent manufactured goods, a significant segment of the US population relates job loss to China's underhanded economic policies and cyber espionage.

Both countries continue to accuse each other, as cyber espionage continues unabated although seemingly at a lower scale, even though the agreement has been hailed as a landmark event due to China's acknowledgement of malicious cyber activities from its territory. Chinese hackers have penetrated defense networks stealing information on numerous weapons programs, including the Patriot missile system, F-35 Joint Strike Fighter. They have also expanded their attention on technology companies, financial institutions, think tanks and others to the extent General Keith Alexander from US Cyber Command claimed that the espionage on American firms and government systems represent the "greatest transfer of wealth in history". He estimated the loss at $250 billion in stolen information and $114 billion in related expenses.[12] China (as does the US)

---

[11] Daniel M. Slane et al, 2010 Report to Congress of the US-China Economic and Security Review Commission, (Washington DC: US Government Printing Office, 2010), 18.
[12] Segal, Adam. "The Hacked World Order." (Public Affairs: New York), 2016.

seems to rely on the attribution challenge to deny any involvement in cyber espionage despite the 2013 Mandiant report identifying PLA 61398 cyber unit actively engaged in cyber attacks.[13] This issue will remain a point of contention, as the US and China do not share the delineation between national security interests and the economy.

The Snowden leaks compounded the confusion over the distinction between national security and economy, as they reveal the US engaging in economic espionage of numerous financial institutions, including Microsoft, the International Monetary Fund, Google, Petrobras, and others. The US justified these operations as routine by creating a linkage to national security. Director of National Intelligence, James Clapper, stated, "…The US does not use foreign intelligence capabilities to steal the trade secrets of foreign companies… on behalf of US companies to enhance their international competitiveness or increase their bottom line."[14] Conversely, stealing to benefit Chinese firms help the nation, as the firms serve to modernize the country and build economic power. The subtle distinction from the US perspective may be problematic for other states as intellectual property related to critical industries may prove valuable to national security. For instance, China may find energy production vital to increasing national energy independence, which translates to economic growth, political stability and regime survival. [4]

The US leveraged its economic significance to China by emphasizing the distinction when in 2014, it indicted five Chinese PLA officers for economic espionage to

---

[13] Mandiant, APT1: Exposing One of China's Cyber Espionage Units. 2013. Last accessed on 15 Apr 2017. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[14] Gary Brown and Christopher Yung, How Washington Approaches Cyberspace and its 2015 Cybersecurity Agreement with China. The Diplomat, 19 Jan 2017. Last accessed on 15 Apr 2017. http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/.

benefit the Chinese domestic firms. Despite objections and China's abrupt disengagement from the bilateral cyber working group, in 2015, China was compelled to sign the Cyber Security Agreement when the US threatened sanctions due to the severity and frequency of the Chinese malicious cyber intrusions. China's willingness to acknowledge the cyber attacks from its territory, not necessarily from its government, reflects the conflation between China's national security interests and economic development. It also indicates China's pragmatism given the importance of the US on the international stage. The agreement is largely viewed as an important step towards a more enforceable and substantive agreement. According to Rand, a US think tank, "The Chinese see cybersecurity talks as a way to appease U.S. irritation more than to achieve anything specific. In contrast, the United States places a much higher emphasis on using such dialogues to resolve cybersecurity issues."[15]

China's discomfort with the US hegemony in cyberspace may impede genuine cooperation. For instance, both countries appreciate the requirement not to attack critical infrastructure, but diverge on conducting cyber espionage on such target due to the attribution problem. Rand contends, "China believes it cannot catch the cheating by the United States and is apprehensive of any agreement that would put them at a[5] corresponding disadvantage."[16] Such fundamental distrust proves challenging to any enforceable framework that holds both countries accountable. China seems hesitant about US intention, as the dichotomy between communism (although China is more of a state-controlled market economy than it is communism), and capitalism (freedom, human

---

[15] Harold, Scott W; Libicki, Martin C; Cevallos, Astrid S. "Getting to Yes With China in Cyberspace." Rand Corporation. Last accessed on 10 Apr 2017. http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf.

[16] Ibid., 12.

rights, etc.) seem to subconsciously control the undertone of any narrative. Furthermore, China views the pivot to Asia as worse than containment and accuses the US of inciting its neighbours to assume a posture of confrontation with China. Therefore, China is protective of its internal affairs and frames the cyber conflicts in terms of sovereignty and national security interests.

Second, US and China approach cyberspace differently in terms of information control and network security. As mentioned, the CCP views US democratic values as antithetical to its fundamental values and therefore a threat to the regime. Dr. John Lindsay from University of Toronto indicated that China views information security as information control, which explains the realignment to the bureau that is in charge of propaganda.[17] The US and west refers to information security as network or cyber security in terms of a robust, secure, and reliable information system. The difference in terminology is worth noting, as an open and secure network is a non-starter during any discussions with China.

The free flow of information in cyberspace may be constraining for the US in terms of abiding by the agreement to address cyber-enabled theft of intellectual property. Conversely, control of the internet infrastructure is already embedded in the Chinese [6]government system, facilitating compliance with the agreement. China's strength may also be a weakness, as denial of malicious activities emanating from its borders may be limited. Dr. Lindsay explained that malicious cyber activities may be facilitated by China's tight governance of the infrastructure, as it focuses on specific sets of criteria that are politically subversive, not necessarily criminal.[18] As a result, hackers

[17] Australian National University, The role of Cyber Security in China Foreign Policy. 23 Feb 2016. Last accessed on 15 Apr 2017. https://www.youtube.com/watch?v=zcO0mIfkYqU.

tend to function with impunity as they prey on the domestic and international community. Despite promoting universal values, many nations are cautious about the US pre-eminence in the cyber ecosystem. General Michael Hayden, former Director of National Security Agency, stated, "When speaking of the (cyber) threat, citizens of the first-world nations were recently asked whom they fear most in cyberspace and the most popular answer was not China or India or France or Israel. It was the United States."[19] China's ambivalence to comply with an agreement regulating the behavior in a domain that was created and mastered by the opposing nation is rational. Thus, a cooperation framework must account for this rationale and establish a governance system that both sides find acceptable.

[7]Unlike the US, China regards privacy and communication rights as destabilizing to the order and structure established by the CCP. Beijing promotes cyber sovereignty to emphasize their right to establish their norms in their own country. President Xi Jinping supports non-interference in China's ability to monitor and restrict internet access, and transforming the global internet governance structure into a multi-lateral, democratic and transparent system; the motive seems pointed at diminishing the US role.[20] China seems constrained by the open internet where democratic ideals may usurp the CCP's authority and inspire dissidence, leading the CCP to install the control mechanisms such as the Great Firewall and the Great Cannon as the intermediary between the open Internet and China. The monitoring and blocking tools provide China situational awareness for

---

[18] Australian National University, The role of Cyber Security in China Foreign Policy. 23 Feb 2016. Last accessed on 15 Apr 2017. https://www.youtube.com/watch?v=zcO0mIfkYqU.

[19] Panayotis Yannakogeorgos and Adam Lowther, Conflict and Cooperation in Cyberspace: The challenge to National Security. (Taylor & Francis Group: Florida), 2014.

[20] Gary Brown and Christopher Yung, China's Cyber Activities (Including Attacks) Closely Mirror How It Conceives of Cyberspace. 19 Jan 2017. Last accessed on 15 Apr 2017. http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity/.

effective administration and management of information within China.

While the philosophy varies significantly, the US is intrigued with the notion of a cyber common operating picture to enable commanders to plan proactively and react effectively to fluid and complex cyber intrusions. General Alexander noted, "We must first understand our networks and build an effective cyber situation awareness in real time through a common, sharable operating picture."[21] The driver is to project power, fight, and defend effectively in the cyber domain. While the thrust is not about information control to the same degree as the Chinese, the concept is similar, as the management of such a complex domain requires vigilance, planning, and preparation. Experts from the U.S. Army Research Laboratory stated, "cyber attacks are adversarial digital ways of determining who gets power, wealth, and resources."[22] Perhaps, this requirement is a common ground from which dialogue with the Chinese can be based.

The perception of cyber threats differs between both countries, which set the stage for more suspicion of each other's intent. The US believes that cyber powers such as Russia and China represent the threat to US critical infrastructure, economic, military and political apparatus. Anthony and Justin Cordesman from CSIS indicated, "Most[8] adversaries will recognize the information advantage and military superiority of the US…they will try to circumvent or minimize US strengths and exploit weaknesses."[23] Conversely, China insists that the US is hypocritical, as it maneuvers the narrative to its

---

[21] Alexander Kott, Cliff Wang, and Robert F. Erbacher, "Cyber Defense and Situational Awareness." (Springer: Switzerland), 2014. 21.

[22] Ibid., 97.

[23] Anthony H. and Justin G.Cordsma, "Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland." (CSIS: Washington D.C.), 2002.

advantage by pushing for cybersecurity cooperation while developing and deploying technologies that threaten the political stability in Russia and China. The suspicion is warranted given the history of US involvement in Chinese internal affairs; however, the economic prowess of both nations and the interdependency of their economy demand mutually-beneficial approaches based on common ground. Suspicion exacerbates the chasm and will likely destabilize the two economic powerhouses with global implications.

[9]US and China share a history of launching accusations at each other, especially when substantial evidence warrants the naming and shaming method. NBC News reported more than 600 American companies were victims of cyber espionage over a five-year period with clusters in the industrial centers.[24] Furthermore, Admiral Mike Rogers, the current Commander of US Cyber Command revealed that despite China's pledge to halt cyber attacks on the US, China continues to target and exploit US government, defense industry and private networks designed to exfiltrate valuable information and map critical computer networks for future attack in a crisis.[25] Admiral Rogers' testimony is consistent with that of former Director of National Intelligence, James Clapper. No definitive evidence seems to link the CCP to the cyber attacks from its territory; however, the CCP is likely connected to a significant portion of the attacks given the motive, the focus of the attacks on the strategically and economically important industries identified by the CCP for growth, the linguistic features in the code analysis,

---

[24] Robert Windrem, Exclusive: Secret NSA Map Shows China Cyber Attack on US Targets. NBC News, 13 Jul 2015. Last accessed on 15 Apr 2017. http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211.

[25] Bill Gertz, China Continuing Cyber Attacks on US networks. The Washington Free Beacon, 18 Mar 2016. Last accessed on 15 Apr 2017. http://freebeacon.com/national-security/china-continuing-cyber-attacks-on-u-s-networks/.

other technical indicators, and investigations discovering the PLA unit behind the attack. China, on the other hand, also claims that its computer networks are often under attack from the US, prompting China to expand resources to constantly protect its networks.

China believes cyber sovereignty is the panacea; however, the implication from a Chinese perspective remains unclear in terms of the meaning of sovereignty and the enforceability measures. Does sovereignty entail kinetic attack, economic sanctions and other coercive measures on the offending country? How would one combat the attribution issue to prevent plausible deniability? What constitutes an act of war? A host of other questions seem to indicate China uses cyber sovereignty as a deflection tool to evade responsibility and accountability for cyber espionage and human rights. As a sovereign nation that promotes a peaceful and responsible rise, and pledges to contribute to international order and security as a member of the United Nations Security Council, China's expectation of non-interference in its internal affairs seems practical. Qin Yaqing, Executive Vice President at China Foreign Affairs University and member of the Central Committee of the CCP revealed that China believes in pragmatic diplomacy and endeavors to cooperate based on commonalities while managing the key differences.[26] The key is to prevent the areas of disagreement from interfering with a collaborative and cooperative framework. [10]

Professor Lindsay offered the following factors as impediments to China in the cybersecurity realm: espionage does not equate to productivity, aggressive doctrine does not lend itself to capability, and lack of governing institution.[27] China has collected exabytes of information, but lacks the institutional framework to convert the data into

---

[26] Qin Yaqing, Managing Sino-US Relations: The Chinese Way. Princeton University, 2008. Last accessed on 16 Apr 2017. https://www.youtube.com/watch?v=vWfJIoVQcfE.

intelligence and productivity. China has driven informatization from the top down, which tends to stifle creativity and promote linear thinking. It is thought next to impossible for China to replicate Silicon Valley given the lack of legal systems, venture capital, recreational opportunities, and institution that foster creativity free of government interference.

The technological revolution in the US started from the bottom up by free-spirited hippies who abhorred government oversight. Silicon Valley is difficult to replicate anywhere let alone in a society strictly controlled by a government that pushes informatization from the top down. Furthermore, China lacks the collaborative organizational structure that can effectively collect and translate the data into intelligence, and process and distribute it to the appropriate people who can integrate it into the economy. That is a challenging and complex endeavor that requires contextual data, innovation, and creativity. In essence, data without context can be useless, as the golden nugget can be a needle in a haystack. This notion, by no means, obviates the need to secure cyberspace and address cybersecurity with China. Despite its shortcomings, China seems to have benefitted from the cyber espionage. Case in point, Microsoft and Cisco were required to disclose their codes to the CCP and in no time domestic companies such as Huawei had deployed routers with similar technology to the international market, introducing significant competition to US firms. [11]

China has developed aggressive doctrines that concentrate asymmetric means to reach parity with a stronger military power. Unrestricted warfare is one such book written by two PLA officers who advocate cyber attacks on websites and financial institutions,

---

[27] John Lindsay, The Role of Cybersecurity in Chinese Foreign Policy. Australian National University, 2016. Last accessed on 16 Apr 2017. https://www.youtube.com/watch?v=zcO0mIfkYqU.

terrorism, urban warfare, media manipulation, and other tactics to compensate for China's military inferiority. "The first rule of unrestricted warfare is that there are no rules with nothing forbidden. Strong countries make the rules while rising ones break them and exploit loopholes."[28] It contends the US is flexible with the rules depending on its purpose, but it cannot break them due to legitimacy on the world stage. Given the modernization of the PLA concentrates on asymmetric capabilities, targeting the reliance of the US military on technology, the doctrine seemingly reflects the principles in the book. However, China lacks the experience and institutions to fight a formidable foe effectively in the cyber domain, especially a foe who invented the domain and has proven capable of conducting combat operations in that ecosystem.

[12]As mentioned before, China views informatization as the requirement to modernize the society and control the information to sanitize the Internet. As a result, the cyber vocabulary is different from the US and West, which can cause unnecessary tension. The fact that the Cyberspace Administration of China answers to the Central Leading Group for Internet Security and Informatization in charge of propaganda reflects the CCP's priority to control the narrative as opposed to securing the network (in a West sense) within China. China has tightened its grip on internet control to prevent dissidents from using sites such as Github, reportedly funded by the US government, that provide instructions on how to bypass the great firewall in China. According to the Economist, the CCP hires 100,000 (other sources note 300,000 to 500,000) people to police China's Internet around the clock based on certain criteria such as no criticism of senior leadership, no organizing to threaten the government, no search of democracy or human

[28] Qiao Liang and Wang Xiangsui, Unrestricted Warfare. Feb 1999. Last accessed on 16 Apr 2017. http://www.c4i.org/unrestricted.pdf.

rights, no pornography, and other prohibited actions.[29] China does not tolerate dissidents or freedom of speech in its territory, but it promotes pragmatism and universal rights on the International stage. This paradox cements misgivings about its true intent despite signing the agreement.

Finally, scrutiny of this agreement asserts that the effectiveness of this agreement is debatable, as implications of the divergent views in cyberspace can have a cascading effect on other aspects of the relationship. RAND report on the agreement sheds light on the rationale behind China's ambivalence based on interviews of officials in China and several experts, "China's own approach to deterrence tends to assume…the most powerful actor or actors in the system will attempt to cover up the differences between its interests and those of other weaker actors."[30] China expects the US to use normative language that promotes cooperation and legitimacy as a pretext to subdue the weaker actors.

[13]China views the norm in cyberspace as a zero-sum game and tends to view the implication as benefits and losses based on power relationships as opposed to right and wrong. China consistently voice opposition to the norms and laws that govern the international system, as they do not reflect China's growing power and status. China

---

[29] E.H., How does China Censor the Internet. The Economist, 22 Apr 2013. Last accessed on 16 Apr 2017. http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-china-censors-internet.

[30] Harold, Scott W; Libicki, Martin C; Cevallos, Astrid S. "Getting to Yes With China in Cyberspace." Rand Corporation. Last accessed on 10 Apr 2017. http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf.

[31] China Daily, International Strategy of Cooperation on Cyberspace. 2 Mar 2017. Last accessed on 16 Apr 2017. http://wap.chinadaily.com.cn/2017-03/02/content_28401127.htm.

[32] Harold, Scott W; Libicki, Martin C; Cevallos, Astrid S. "Getting to Yes With China in Cyberspace." Rand Corporation. Last accessed on 10 Apr 2017. http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf.

considers the norms reflective of the interests of the hegemonic powers as opposed to the international community. In short, China wants a seat at the table as indicated by its new International Strategy of Cooperation in Cyberspace where President Jinping advocates for a multi-lateral governance. The Strategy states, "The United Nations, as an important channel, should play a leading role in coordinating the positions of various parties and build international consensus."[31] The strategy also calls for an open, secure, cooperative, and orderly cyberspace. The word 'orderly' supports China's and Russia's cyber sovereignty, which aims to relieve pressure from western countries about human rights and coercive control within their territory. China seems to be using normative language as well to reinforce and legitimize its current practices.

China is concerned about the fact that the US government is immune to sanctions, giving China no leverage in any agreements. China's assertion is consistent with the obsession to emerge from the 'century of humiliation' to instill national pride and avert interference from foreign powers that cause China to collapse into civil war. Thus, any agreement with the Chinese must account for their values and present them in a powerful and positive light on the international stage. According to Brookings Institution, "There are 4 billion people behind the 50 billion devices that connect to the Internet. They send more than 90 trillion emails a year and conduct more than two trillion transactions."[32] Cyberspace is valuable, but the optics must avert Chinese acquiescence to a stronger power.

It stands to reason that the agreement has no substance. In 2014, The US has shown good faith by distancing itself from the Internet Corporation for Assigned Names and Numbers, which is a non-profit organization that coordinates the maintenance and

procedures of the databases of Internet names and numbers world-wide. China is clearly not satisfied as evidenced by its proposal for a multi-lateral governance structure. To be fair, 10 of the 13 root servers that enable the Internet to function reside in the US, which likely raised suspicion that the US continues to dominate the cyber domain.

**Cooperative Framework**

The security dilemma in the cyber domain from a realist perspective can be destabilizing, but pragmatism will ultimately prevail as both countries will tolerate malicious events up to a significant threshold due to the economic impact. President Obama reiterates that US foreign policy is based on pragmatism as opposed to realism or idealism given the disorder in the world.[33] Recently US President Trump decided not to label China as a currency manipulator, despite obvious evidence, to enlist its cooperation on dealing with North Korea. The complex realities of geopolitics demand cooperation in the quest for influence, even if it means the agreement is more symbolic than substantive.

[14]A cooperative framework should leverage the Tallinn Manual 2.0, which establishes international regulatory cyberspace norms similar to the law of armed conflict from the Geneva Conventions. Brookings Institution asserted that US-China cooperation on cyber would "bolster US-China bilateral relations, serve as a crucial building block for multi-lateral efforts in the cyber arena, and also aid on broader… engagement on issues of importance such as global finance and the environment."[34] The report estimates 55,000 new malwares each day and 200,000 computers are turned into zombies, which means

[33] Barack H. Obama, Obama on American Politics and Economy: The Extended Voxx Conversation. 9 Feb 2015. Last accessed on 16 Apr 2017. https://www.youtube.com/watch?v=RBKhpV6MYto.
[34] Kenneth Lieberthal and Peter W. Singer, Cybersecurity and US-China Relations. Feb 2012. Last accessed on 15 Apr 2017. https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf

the cyberspace threat is pervasive and dynamic. The urgency and amorphous nature of cyber requires cooperation to prevent miscalculation and address the criminal actions.

Both countries must accept their right to develop and deploy cyber capabilities to support military espionage and to respect their political differences in terms of human rights and freedom of expression. Brookings proposed the following cooperative measures: expand engagement to a large scale, focus on common areas of interest such as crime, address the key principles (even in the intractable areas) to enhance understanding, hold open and honest discussion of the existing norms in the global institution to identify areas of agreement, account for the red lines, and clarify the attribution issue. The framework cannot be rushed, as it lays the foundation for mutual trust.

Given the innovative spirit of the Americans and the West encouraged by an open and democratic system, a normalized and cooperative relationship with China is more likely to influence China than an antagonistic narrative that seems to threaten its foundation. Thus, the US must resume a frequent US-China cyber-working group that comprises influential and knowledgeable delegates immersed into each other's decision calculus, culture and history to ensure transparency, and trust in developing norms that can survive international scrutiny. Second, the US government must engage with Canada and the corporations to develop a proactive and effective cyber defense of their critical infrastructure. The idea is to significantly reduce vulnerabilities given the interdependencies of the countries' economies and harden the cyber battlespace to make it more challenging for China and Russia's offensive cyber capabilities. A perplexed environment will likely induce Chinese cooperation and suppress nationalism. Otherwise, China stands to gain more from covert cyber economic and military espionage than

cooperation. Third, the US must include measurable enforcement and verification measures that respect China's sovereignty while discouraging and reducing cyber violations from their territory. Finally, The US must retain some leverage such as economic or diplomatic sanctions that persuade China to address cyber intrusions, given the linkage between economic and political stability to regime survival.

## Conclusion

The existing 2015 US-China Cyber Security Agreement merely represents China's acknowledgement of significant cyber security intrusions from its territory and not necessarily the CCP being complicit in economic espionage. Scrutiny of the agreement yields no substance as evidenced by the conflicting views of the relationship between national security interests and the economy, the divergent approaches to cyberspace, and the non-measurable and unverifiable measures of effectiveness. The historical narratives, geopolitical interests, and ideological constraints underline China's pragmatic approach in terms of advocating a cyberspace governance structure that weakens the US dominance in that sphere under the guise of a normative message based on open and democratic structure that gives a voice to all countries. China also pushes for cyber sovereignty to reduce the threat posed by the US democratic ideals such as freedom of expression and universal human rights.

The pernicious impact of a destabilizing US-China relationship on the world economy requires a cooperative framework that reduces mistrust and conflict. Cyber has become weaponized to the extent it can cripple an economy, critical infrastructures, and command and control systems where nations become entangled in a security dilemma

that will likely induce escalation. US and China, among many other nations, are equipped with potent offensive cyber capabilities that require a cooperative framework to ensure mutual trust, acknowledge their right to espionage, accept the fundamental differences, and plow ahead on areas of common interests on which norms can be based that withstand international scrutiny.

The US must cooperate with other like-minded nations and western corporations to develop a robust cyber defense of their critical infrastructure and create a non-permissive environment for Chinese offensive cyber capabilities. The structure must involve an interconnected cyber common operational picture that provides shared situational awareness and a mechanism that fosters coordinated and proactive cyber response. The idea is to dissuade China's illicit cyber exploitation and flipped the decision calculus where cooperation is advantageous. The narrative must drive cooperation versus antagonism, so frequent bilateral cyber working groups with the appropriate expertise is critical to developing a more comprehensive agreement.

## BIBLIOGRAPHY

Clark, Richard A; Knake, Robert A. “Cyber War: The Next Threat to National Security and What to Do About It.” (Harper Collins: New York), 2010.

Auerbach Publications. “Conflict and Cooperation in Cyberspace.” (Taylor & Francis Group: New York), 2014.

Obama, Barack H. “Obama on American Politics and Economy: The Extended Voxx Conversation.” 9 Feb 2015. Last accessed on 16 Apr 2017. https://www.youtube.com/watch?v=RBKhpV6MYto.

Stevens, Tim. “Cyber Security and the Politics of Time.” (Cambridge University: London), 2016.

Brookings Institution, “China’s Security and Foreign Policies: Comparing American and Japanese Perspectives.” Last accessed on 30 October 2016, https://www.youtube.com/watch?v=f2Nh-tu2FUI

Valeriano, Brandon and Maness, Ryan C. “Cyber War versus Cyber Realities.” (Oxford University: New York), 2015.

Bergsten, Fred C; Freeman, Charles; Lardy, Nicholas R; Mitchell, Derek J. “China’s Rise: Challenges and Opportunities.” (CSIS: Washington, D.C.), 2008.

Huaxia. “China’s Five Year Plan to Benefit the World.” Xinhua, 3 Nov 2015. Last accessed on 14 Apr 2017. http://news.xinhuanet.com/english/2015-11/03/c_134780397.htm

China Daily, International Strategy of Cooperation on Cyberspace. 2 Mar 2017. Last accessed on 16 Apr 2017. http://wap.chinadaily.com.cn/2017-03/02/content_28401127.htm.

Inkster, Nigel. “China’s Cyber Power.” (Bell & Bain Ltd: Glasgow), 2016.

Harold, Scott W; Libicki, Martin C; Cevallos, Astrid S. “Getting to Yes With China in Cyberspace.” Rand Corporation. Last accessed on 10 Apr 2017. http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf.

Bryan Krekel, Patton Adams, George Bakos. “Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. 7 Mar 2012. Last accessed on 10 Apr 2017. https://www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf.

United States Government, “International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World,” May 2011, 14.

Carr, Jeffrey. “Inside Cyber Warfare” (O’Reilly Media: California), 2010.

Segal, Adam. “The Hacked World Order.” (Public Affairs: New York), 2016.

Kremer, Jan-Frederick and Mueller, Benedikt (editors). “Cyberspace and International Relations: Theory, Prospects and Challenges.” (Springer-Verlag: Germany), 2014.

Lindsay, John. “The Role of Cybersecurity in Chinese Foreign Policy.” Australian National University, 2016. Last accessed on 16 Apr 2017. https://www.youtube.com/watch?v=zcO0mIfkYqU.

2010 Report to Congress. “US-China Economic and Security Review Commission.” (U.S. Government Printing Office: Washington D.C.), 2010.

Lieberthal, Kenneth and Singer, Peter W. “Cybersecurity and US-China Relations.” Brookings Institution, Feb 2012. Last accessed on 15 Apr 2017. https://www.brookings.edu/wpcontent/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf.

Richet, Jean-Loup. “Cybersecurity Policies and Strategies for Cyberwarfare Prevention.” (IGI Global: Pensylvania), 2015.

Singer, P.W. and Friedman, Alan. “Cybersecurity and Cyberwar. What Everyone Needs to Know.” (Oxford University Press: UK), 2014.

Reveron, Derek S. “Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World.” (Georgetown University Press: Washington D.C.), 2012.

The White House, “FACT SHEET: President Xi Jinping’s visit to the United States,” September 25 2015, last accessed May 2 2016. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

Clapper, James A quoted in Franz-Stefan Gady, “Top US Spy Chief: China Still Successful in Cyber Espionage Against US,” *The Diplomat*, February 16 2016, last accessed May 2 2016. http://thediplomat.com/2016/02/top-us-spy-chief-china-still-successful-in-cyber-espionage-against-us/

Kiggins, Ryan D. “US Leadership in Cyberspace: Transnational Cyber Security and Global Governance,” in *Cyberspace and International Relations: Theory, Prospects and Challenge*, eds. Benedikt Muller and Jan-Frederik Kremer (Berlin: Springer, 2004), 163.

Yaqing, Qin. “Managing Sino-US Relations: The Chinese Way.” Princeton University, 2008. Last accessed on 16 Apr 2017. https://www.youtube.com/watch?v=vWfJIoVQcfE.

Communications Security Establishment. “Minister Sajjan delivers key note address at the 2016 SNIT IT Security Entrepreneurs Forum.” Government of Canada. Last accessed on 31 January 2017. https://www.cse-cst.gc.ca/en/media/media-2016-04-22.

Lieutenant General Bender, William J. “United States Air Force Information Dominance Vision.” (2016). Last accessed on 31 January 2017. http://www.safcioa6.af.mil/Portals/64/documents/AFD-150112-026.pdf?ver=2016-07-22-144347-233.

Kott, Alexander; Wang, Cliff; and Erbacher, Robert F. “Cyber Defense and Situational Awareness.” (Springer: Switzerland), 2014.

The Honourable Toews, Vic. “Canada Cyber Security Strategy—For a Stronger and \ More Prosperous Canada.” Government of Canada (2010). Last accessed on 31 January 2017. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

Friis, Karsten and Ringsmose, Jens. “Conflict in Cyber Space: Theoretical, Strategic and Legal Prespectives.” (Routledge: New York), 2016.

Cordesman, Anthony H and Gordesman, Justin G. “Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland.” (CSIS: Washington D.C.), 2002.

Ventre, Daniel. “Cyber Conflict: Competing National Perspectives.” (ISTE Ltd: London), 2012.

Campen, Alan D. and Dearth, Douglas H. “Cyberwar 3.0: Human Factors in Information Operations and Future Conflict.” (AFCEA International Press: Virginia), 2000.

Welsh, William. “Cyber Warrior--The Next Generations.” Defense System (2014) Last accessed on 31 January 2017. https://defensesystems.com/articles/2014/01/23/next-generation-cyber-warriors.aspx.

Moens, Alexander; Cushing, Seychelle; and Dowd, Alan W. “Cyber Security Challenges, Fraser Institute.” Fraser Institute (2015). Last accessed on 1 February 2017. https://www.fraserinstitute.org/sites/default/files/cybersecurity-challenges-for-canada-and-the-united-states.pdf.

Communications Security Establishment. “Minister Sajjan delivers key note address at the 2016 SNIT IT Security Entrepreneurs Forum.” Government of Canada. Last accessed on 31 January 2017. https://www.cse-cst.gc.ca/en/media/media-2016-04-22.

Ducheine, Paul; Osinga, Frans; Soeters, Joseph. 'Cyber Warfare: Critical Perspectives.' (Asser Press: Hague), 2012.

Boutilier, Alex. "Cyber Security Review Still in Early Days—Public Security Official Tells Senate." The Star (2016). Last accessed on 1 February 2017. https://www.thestar.com/news/canada/2016/03/07/cyber-security-review-still-in-early-days-public-security-officials-tell-senate.html.

Raymond, David; Cross, Tom; Conti, Gregory; and Nowatkowski, Michael. "Key Terrain in Cyberspace: Seeking the High Ground." International Conference on Cyber Conflict (2014) https://ccdcoe.org/sites/default/files/multimedia/pdf/d2r1s8_raymondcross.pdf.

Liang, Qiao and Xiangsui, Wang. "Unrestricted Warfare." Feb 1999. Last accessed on 16 Apr 2017. http://www.c4i.org/unrestricted.pdf.

Windrem, Robert. "Exclusive: Secret NSA Map Shows China Cyber Attack on US Targets." NBC News, 13 Jul 2015. Last accessed on 15 Apr 2017. http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211.

Gertz, Bill. "China Continuing Cyber Attacks on US networks. The Washington Free Beacon." 18 Mar 2016. Last accessed on 15 Apr 2017. http://freebeacon.com/national-security/china-continuing-cyber-attacks-on-u-s-networks/.

Brown, Gary and Yung, Christopher. "China's Cyber Activities (Including Attacks) Closely Mirror How It Conceives of Cyberspace." 19 Jan 2017. Last accessed on 15 Apr 2017. http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2chinas-take-on-cyberspace-and-cybersecurity/.

Mandiant. "APT1: Exposing One of China's Cyber Espionage Units." 2013. Last accessed on 15 Apr 2017. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Xu, Beina. "South China Sea Tensions." Council on Foreign Relations, 14 May 2014. Last accessed on 15 Apr 2017. http://www.cfr.org/china/south-china-sea-tensions/p29790.