NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

2015 U.S.–CHINA CYBER AGREEMENT: A NEW HOPE, OR "THE EMPIRE STRIKES BACK"?

by

Joseph B. M. Chua

December 2017

Thesis Advisor: Wade Huntley
Second Reader: Michael Glosny

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE 2015 U.S.–CHINA CYBER AGREEMENT: A NEW HOPE, OR "THE EMPIRE STRIKES BACK"?	**5. FUNDING NUMBERS**
6. AUTHOR(S) Joseph B. M. Chua	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

On September 25, 2015, President Barack Obama and President Xi Jinping announced the formation of a U.S.–China Cyber Agreement. After years of suspected cyber-enabled economic espionage, many analysts considered the Agreement a surprising and welcome development. Still, other analysts remained pessimistic as to the Agreement's potential impact in changing behavior, predicting Chinese behavior would remain unchanged or be altered in a way that would not significantly reduce the level of cyber espionage instances or damages. Given the two years since the signing of Agreement, this thesis examines data from pre- and post-Agreement periods for potential trends and impacts, to address the question, "How have the results of the 2015 U.S.–China Cyber Agreement impacted the prospects of future U.S.–China cooperation in cyberspace?" To evaluate this question, this thesis first examines data from FireEye, Hackmageddon, and other cybersecurity organizations, which report the volume of attacks and other relevant trends. This thesis then repurposes the Schmitt Analysis to provide an alternative and more comprehensive perspective of China's compliance with the Agreement. Last, this thesis surveys Chinese policies from the pre- and post-Agreement periods, highlighting notable differences.

After examination of the data, this thesis finds that the Agreement, though likely not a "watershed moment," played a significant role in accelerating Chinese behavior toward a reduction in the level of attacks. Data from FireEye, Hackmageddon, and other cybersecurity organizations suggests a genuine effort on the part of the Chinese to comply with the Agreement. Additionally, data examined by repurposing the Schmitt Analysis supports similar findings. Furthermore, Chinese policies appear to have shifted following the Agreement, toward a cyber posture more consistent with U.S. aspirations. In sum, the Agreement plays a significant role toward fostering more friendly U.S.–China cyber relations.

14. SUBJECT TERMS United States, China, cyber, cyber agreement, FireEye, Hackmageddon, Schmitt Analysis, cyberattack, cyber policy, Chinese policy	**15. NUMBER OF PAGES** 169
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

2015 U.S.–CHINA CYBER AGREEMENT:
A NEW HOPE, OR "THE EMPIRE STRIKES BACK"?

Joseph B. M. Chua
Lieutenant, United States Navy
B.A., B.S., University of California, Davis, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(FAR EAST, SOUTHEAST ASIA, THE PACIFIC)

from the

NAVAL POSTGRADUATE SCHOOL
December 2017

Approved by: Wade Huntley, Ph.D.
Thesis Advisor

Michael Glosny, Ph.D.
Second Reader

Michael Glosny, Ph.D.
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

On September 25, 2015, President Barack Obama and President Xi Jinping announced the formation of a U.S.–China Cyber Agreement. After years of suspected cyber-enabled economic espionage, many analysts considered the Agreement a surprising and welcome development. Still, other analysts remained pessimistic as to the Agreement's potential impact in changing behavior, predicting Chinese behavior would remain unchanged or be altered in a way that would not significantly reduce the level of cyber espionage instances or damages. Given the two years since the signing of Agreement, this thesis examines data from pre- and post-Agreement periods for potential trends and impacts, to address the question, "How have the results of the 2015 U.S.–China Cyber Agreement impacted the prospects of future U.S.–China cooperation in cyberspace?" To evaluate this question, this thesis first examines data from FireEye, Hackmageddon, and other cybersecurity organizations, which report the volume of attacks and other relevant trends. This thesis then repurposes the Schmitt Analysis to provide an alternative and more comprehensive perspective of China's compliance with the Agreement. Last, this thesis surveys Chinese policies from the pre- and post-Agreement periods, highlighting notable differences.

After examination of the data, this thesis finds that the Agreement, though likely not a "watershed moment," played a significant role in accelerating Chinese behavior toward a reduction in the level of attacks. Data from FireEye, Hackmageddon, and other cybersecurity organizations suggests a genuine effort on the part of the Chinese to comply with the Agreement. Additionally, data examined by repurposing the Schmitt Analysis supports similar findings. Furthermore, Chinese policies appear to have shifted following the Agreement, toward a cyber posture more consistent with U.S. aspirations. In sum, the Agreement plays a significant role toward fostering more friendly U.S.–China cyber relations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AGREEMENT	2015 U.S.-China Cyber Agreement
CCP	Chinese Communist Party
CICIR	Cooperation in Cybersecurity China Institute of Contemporary International Relations
CNA	Computer Network Attack
CSIS	Center for Strategic and International Studies |
CWG	Cyber Working Group
FMPRC	Ministry of Foreign Affairs of the People's Republic of China
GGE	Group of Government Experts
HTTP	Hypertext Transfer Protocol
ISTR	Internet Security Threat Report
NSA	National Security Agency
NPT	Nonproliferation Treaty
OPM	Office of Personnel Management
OSI	Open Systems Interconnection
PRC	People's Republic of China
RAT	Remote Access Tool
SALT	Strategic Arms Limitation Treaty
SCIO	Information Office of the State Council of the People's Republic of China
TFP	Total Factor Productivity
TLS	Transport Layer Security
TTP	Tools, Techniques, and Procedures
USCC	US-China Commission

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I'd like to thank my wife, Pearl, without whom much of my success wouldn't be possible. I love you and I'm excited for the future in front of us.

I'd also like to thank my family. To my parents, step-parents, and siblings, thank you for putting up with me for all these years and for all your help along the way. I know I would never have gotten this far without your love and support. To my new in-laws, thank you for helping me as I beat my head against the wall, comfortably of course, in doors, while you guys did the heavy lifting outside. Also, thank you to everyone for helping Pearl and me get through our wedding in the middle of all of this. I couldn't have asked for more.

To my friends, thanks for all the crazy memories and for being my outlet through some of my worst times. Who knew back then that we'd be where we are. Panther pride (I still have the PE shorts somewhere), bro-circle, and team 4PM, thanks for the support.

A special thank you goes to Mrs. Miyahara. Sorry for all of the trouble and immaturity you had to put up with. For me, you are the very embodiment of a teacher, guiding all of us, kicking and screaming, through some of the most tumultuous (SAT word!) periods of our lives. Thank you.

Last, but not least, to my NPS professors and faculty, thank you. To my thesis advisors, Dr. Wade Huntley and Dr. Michael Glosny, I've never been so intellectually intimidated and challenged, and for that, I thank you. You both pushed me to seek knowledge beyond what I thought was my capability. Thanks for not letting me stay within what I thought were my limits. To Dr. Robert Weiner, thank you for walking me through how to survive in graduate school and the thesis process. It was a tough learning curve, but you made the transition manageable. To Carla Hunt, I'm not really sure I'd know how to write a paper if you weren't there. You read almost every one of my papers and helped make them coherent.

I am extremely grateful to all of you. Thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION AND MAIN FINDINGS

How have the results of the 2015 U.S.–China Cyber Agreement impacted the prospects of future U.S.–China cooperation in cyberspace?

During a 2015 summit, President Barack Obama and President Xi Jinping "exchanged views on a range of global, regional, and bilateral subjects."[1] One area of particular interest was the "cybersecurity issue."[2] Both presidents expressed their growing concerns of "cyber-threats" and the need for China and the United States to work together as the "two major cyber countries."[3] Consequently, the two reached a cooperative agreement, also known as the 2015 U.S.-China Cyber Agreement (Agreement), which helped clarify the role of states with cyber espionage.[4]

A significant milestone for U.S.–China relations, the Agreement also represented an important step forward in establishing universal cyber laws and norms; however, as President Obama noted, the actual actions following the agreement dictate much of the scope of the Agreement's impact and implications. Accordingly, this thesis assesses the actual actions taken following the Agreement and examines the implications of the Agreement for both the evolving U.S.–China relationship and the future prospects for cooperation and norm development in cyberspace. More specifically, this thesis explores the following questions. What actions have the U.S. and China taken that can be attributed to the Agreement and what impacts have those actions produced? Do these impacts have broader implications?

---

1 "FACT SHEET: President Xi Jinping's State Visit to the United States," *The White House*, September 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states; "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," *The White House*, September 25, 2014, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

2 "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference."

3 Ibid.

4 Ibid.

Overall, this thesis finds that the Agreement played a significant role in altering Chinese behavior, but was not necessarily a pivotal turning point. The Agreement emerged as part of a wider swath of changes between the United States and China. In terms of the volume of cyberattacks, data from FireEye showed that the number of cyberattacks on the United States attributed to China was declining prior to the Agreement. The Agreement, however, accelerated and stabilized the decline; post-Agreement numbers showed a greater rate of decline and less variation from month to month. Furthermore, utilizing an adapted method of analysis derived from the Schmitt Analysis suggests similar results. Cyber-attacks by China are becoming less damaging and the United States is getting better at tying attacks to China. Last, changes in Chinese cyber policies also suggest a broader shift in Chinese behavior. Post-Agreement changes in Chinese policies suggest a trend toward stronger U.S.-China cyber relations. Additionally, new cybersecurity laws suggest a change in Chinese perceptions of cyberspace more closely aligned with U.S. perceptions. Thus, there is significant evidence to be optimistic and that the Agreement may play a key role in solidifying U.S.-China cyber relations.

Alternatively, however, the evidence also suggests a necessity for the United States to progress cautiously. Data from Matt Tait and other analysts suggest that punitive measures by the United States more accurately represent the cause for the changes in Chinese behavior. Evidence under other criteria from the Schmitt Analysis also suggest reason to progress cautiously as the focus of Chinese cyberattacks shifts towards civilian versus military targets. Changes in Chinese policies may also just be an excuse for the CCP to establish tighter control of cyberspace. These potential spoilers, however, do not completely offset or undermine the evidence to see developments optimistically. For example, while the declining trend of the volume of cyberattacks could quickly reverse, that change has yet to occur. As a result, the United States should focus on what is happening rather than what might happen. In the end, this thesis recommends the United States progress with cautious optimism.

B. SIGNIFICANCE OF THE RESEARCH QUESTION

Prior to the Agreement, the relationship between the United States and China on cyberspace can best be described as contentious.[5] Starting in 2007, allegations of cyberattacks from China on the United States began to emerge, sparking the first embers of tension between the two.[6] Tensions continued to escalate through 2012 following attacks on several U.S. companies like Google, Lockheed Martin, and RSA, all of which seemed to come to a boiling point in 2013 with two events.[7] Mandiant, a cybersecurity firm now part of FireEye, released a report directly implicating China's involvement in cyberattacks; and Edward Snowden released a massive leak of classified information that implicated the National Security Agency's (NSA) involvement in attacks of their own.[8] Both sides appeared to face culpability for escalating cyberattacks, which some analysts saw as the makings of a cyber war.[9]

Following the years of mutual accusations and buildup of tensions, relief did come. In April 2013, the two sides agreed to work cooperatively to address cyber issues, breaking the cycle of escalation. For that purpose, they agreed to establish a cybersecurity working group.[10] Cooperative efforts, however, were short-lived. After the U.S. Justice Department indictment of five PLA officers, China suspended the working group, ending the only formal cooperative link between the two.[11] Consequently, in April 2015, it came

---

[5] Scott Warren Harold, Martin C. Libicki, and Astrid Cevallos, *Getting to Yes with China in Cyberspace* (Santa Monica, CA: RAND Corporation, 2016), http://www.rand.org/pubs/research_reports/RR1335.html.

[6] Amy Chang, "Warring State: China's Cybersecurity Strategy," Center for a New American Security, December 2014, http://cfcollegefoundation.ca/wp-content/uploads/2016/08/CNAS_WarringState_Chang.pdf.

[7] Shashank Bengali, Ken Dilanian, and Alexandra Zavis, "Timeline: Chinese Cyber Attack Disclosures," *Los Angeles Times,* June 5, 2013, http://timelines.latimes.com/la-fg-china-cyber-disclosures-timeline/.

[8] Chang, "Warring State."

[9] "The U.S. vs. China: A Very Civil (Cyber) War," InfoSecurity, June 26, 2012, https://www.infosecurity-magazine.com/magazine-features/the-us-vs-china-a-very-civil-cyber-war/.

[10] Robert O'brien and Shiran Shen, "Cybersecurity between the United States and China," Policy Innovations, May 28, 2013, accessed March 11, 2017, http://www.policyinnovations.org/ideas/commentary/data/000260.

[11] Chang, "Warring State."

as no surprise when President Obama issued an Executive Order declaring a "national emergency" and authorizing sanctions to deal with the threat of "significant malicious cyber-enabled activities."[12] Cooperation failed, sending the two sides back towards an escalating spiral of retaliation. So, when the Agreement was announced at the end of 2015, it came as a surprise that both sides were still willing to act cooperatively.[13]

Cooperation between the United States and China has the potential to shape global cyber norms and, in turn, further development of international law on cyberspace. The two nations, arguably, represent the largest and most significant powers. They have the top two GDPs in the world with a combined GDP (in 2016, in USD) of nearly $30 trillion.[14] Comparatively, the next 16 economies combined are still less than that.[15] Additionally, both have the top two militaries in terms of spending and, arguably, strength.[16] Furthermore, because both nations' ideologies and political structures are diametrically opposed, their cooperation lends itself to a degree of legitimacy on the global stage. If the United States and China can work together and establish norms on an issue, the rest of the world may follow suit.

By analyzing the Agreement and the actions taken since, this thesis provides insight into the future outcomes and implications the Agreement has on the international community and towards shaping norms in cyberspace.

C. LITERATURE REVIEW

Given the recentness of the Agreement, few scholarly articles analyzing the results of the Agreement exist. Analysts, however, provide a wide array of perspectives

---

12 "Executive Order—"Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," *The White House,* April 1, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

13 Harold, Libicki, and Cevallos et al., *Getting to Yes with China in Cyberspace*, 79.

14 "List of Countries by Projected GDP," List of Countries by Projected GDP 2016, StatisticsTimes, accessed February 1, 2017, http://statisticstimes.com/economy/countries-by-projected-gdp.php.

15 Ibid.

16 Jeremy Bender and Skye Gould, "The 35 Most Powerful Militaries in the World," *Business Insider* (July 10, 2014), accessed February 1, 2017, http://www.businessinsider.com/35-most-powerful-militaries-in-the-world-2014-.

of the issues surrounding the Agreement. This literature gives a review of those perspectives to lay background information necessary to address the research question. The literature review is divided into four parts: 1) the "'Cyber Problem' in U.S.-China Relations," 2) current evaluations of the Agreement, 3) potential areas to better measure/evaluate the Agreement, 4) broader impacts.[17]

1. The Cyber Problem in U.S.-China Relations

While scholars agree that there is a cyber problem between the United States and China, there is not a universal consensus of what the problem is. Scholars offer an array of analysis and perspectives of the problems the two sides faced. In general, interpretations of U.S.-China cyber relations mainly vary in terms of which country is seen as more responsible for aggravating cyber activities. This section provides details of the different perspectives.

a. China's Fault

Many analysts argue the dilemma is one of a competing perspective between the United States and China. From a U.S. perspective, China is the aggressor and the main culprit behind attacks.[18] Incidents like the ones listed in "Cyber Incidents Attributed to China" by Laura Saporito and James Lewis in seem to support the *China's fault* view.[19] Mandiant's report, "APT1: Exposing One of China's Cyber Espionage Units," further confirms these views by not only tracing attacks back to specific individuals, but also the locations and desktop screenshots of the attacker's computer.[20] While neither is indisputable proof of the Chinese government operating as the aggressor, the evidence seems to suggest a little more than coincidence.

---

[17] Harold Libicki, and Cevallos et al., *Getting to Yes with China in Cyberspace*.

[18] Ibid.

[19] Laura Saporito and James A. Lewis, *Cyber Incidents Attributed to China,* report, CSIS, March 11, 2013, accessed February 15, 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130314_Chinese_hacking.pdf.

[20] M. I. Center, "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, Tech. Rep, Tech. Rep., 2013.

Mandiant's report, in particular, provided several details that make attribution to China quite specific. The evidence details APT1's pattern of activity and the trail back to PLA Unit 61398.[21] The report also ties China's motives to APT1 as the cyberattack victims are all companies in industries listed as critical to China's strategic plans, including China's "12th Five Year Plan."[22] Mandiant also provides even more incriminating details by identifying specific actors by name and provides minute details, like the tools used and the sheer size necessary to launch some of the attacks that attribution is beyond reproach.

The indictment by the U.S. District Court also supports Mandiant's findings. While presenting much of the similar data like IP addresses, the indictment also provides a list of incidents with dates and the associated actor responsible for the attack.[23] While China, and other critics, may argue that the evidence is circumstantial and lacking definitive proof, the specificity, sources, and thoroughness of the evidence leave little doubt regarding China's behavior in cyberspace.

b. U.S. Is a Threat

From China's perspective, however, China is the victim.[24] China argues it faces a greater threat and problem of cyberattacks, and the United States is one of the aggressors. China argues that the United States is the overwhelming hegemonic power. One particularly strong view is that the United States has an overwhelming advantage in cyberspace, notably in access, research, and development of cyber technologies.[25] These views claim there is clear disparity in power and that the United States is the only one capable of attributing cyberattacks to a particular actor. Furthermore, China is not only

---

[21] M. I. Center, "APT1: Exposing One of China's Cyber Espionage Units."

[22] Ibid.

[23] United States of America vs Wang Dong, Sun Kailing, Wen Xinyu, Huang Zhenyu, Gu Chunhui, no. 14–118 (PA, District Ct, Western District May 1, 2014), https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

[24] Harold et al., *Getting to Yes with China in Cyberspace*, 8.

[25] Melissa E. Hathaway, *Strategic Advantage: Why America Should Care About Cybersecurity*, report, October 2009, accessed February 15, 2017, http://www.belfercenter.org/sites/default/files/legacy/files/Hathaway.Strategic%20Advantage.Why%20America%20Should%20Care%20About%20Cybersecurity.pdf .

incapable of attribution, but as a developing nation, is "the single largest victim of cyber crime and hacking in the world."[26] In sum, their view is the United States is strong and China is weak.[27]

Scholars note that China could also have other possible motives. Some point to a lack of trust in China, implying "things would be much better if the United States trusted China more."[28] Under this perspective, the Agreement could be a tool to help stem unwarranted criticism and accusations aimed at China. One of the most pressing concerns is the issue of China's sovereignty in cyber space. As President Xi alluded to during the 2014 World Internet Conference, like any other territorial domain (air, land, and sea), cyberspace, too, contains "sovereign 'virtual territory.'"[29] Whereas the U.S. believes in a boundary-less cyberspace, for the Chinese, there is an underlying "assumption that the cyberspace is the natural extension, or a new dimension, of national sovereignty."[30] Since people and computers exist in the physical world, so does cyberspace. Connecting to the Internet requires physical connections like routers and computer servers, and it is these physical connections over which states can exert their authority.[31] For instance, like going over bridges, Internet users must go across certain "bridges" to cross from one area to another, and it is a collection of these bridges that form the Internet as a whole. As a result, the bridges themselves along with the people crossing the bridges are the responsibility of the bridge owners. The owners, as this Chinese argument about cyberspace would go, have a right and responsibility to ensure the safety of the users. At

---

[26] Michael Sulmeyer and Amy Chang, "Three Observations on China's Approach to State Action in Cyberspace," *Lawfare* (web blog), January 22, 2017, https://www.lawfareblog.com/three-observations-chinas-approach-state-action-cyberspace.

[27] Ibid.

[28] Ibid.

[29] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor, no.* 42 (Fall 2013), http://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf; Li Yan, "Reforming Internet Governance and the Role of China," *Focus Asia,* no. 12 (February 2015): 1–12, http://isdp.eu/content/uploads/publications/2015-LiYan-Reforming-Internet-Governance-and-the-role-of-China.pdf.

[30] Liu Yangyue, "China's Perspective on Cyber Security," in "Perspectives on Cybersecurity," *Explorations in Cyber International* Relations (Cambridge: Massachusetts Institute of Technology, 2015), 51, https://ecir.mit.edu/sites/default/files/documents/SSRN-id2734336-6.pdf.

[31] Ibid.

the same time, however, users are also subject to the rules and laws of the individual or state owners.

Therefore, from the Chinese perspective, U.S. actions and rhetoric are outlandish and hypocritical. U.S. claims that authoritarian controls over information are oppressive measures ignore the state's role of "raising the ideological and moral standard of the citizens."[32] As the "bridge" owner, the state, or the CCP in this instance, has a duty to protect and guide its people using the bridges. Furthermore, China also refutes U.S. accusations, claiming themselves as the "victim of severe U.S. cyber theft, wiretapping and surveillance activities."[33] In the view of the Chinese, the U.S. is hypocritical, calling China the bully while possessing "'monopolistic advantages' [longduan youshi]" and possessing the true hegemonic power.[34] Thus, the Agreement may be a way to protect Chinese citizens.[35]

2. Current Evaluations of the Agreement

Despite the recentness of the Agreement, several scholars have offered some early evaluations, which to date, mainly vary in terms of the degree to which it has had any impact at all. At one end, some scholars argue preliminary results of the Agreement provide evidence to be optimistic for U.S.-China cyber cooperation. At the opposite end, other scholars argue the results so far are minimal, and so are reason to be pessimistic. This section outlines the arguments presented by both ends as well as the more moderate views in between.

---

[32] Swaine, "Chinese Views on Cybersecurity in Foreign Relations," 5.

[33] "China Reacts Strongly to U.S. Announcement of Indictment Against Chinese Personnel," Ministry of Foreign Affairs of the People's Republic of China, May 20, 2014, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/t1157520.shtml.

[34] Scott Warren Harold, Martin C. Libicki, and Astrid Cevallos, *Getting to Yes with China in Cyberspace* (Santa Monica, CA: RAND Corporation, 2016), 9, http://www.rand.org/pubs/research_reports/RR1335.html.

[35] Gary Brown and Christopher Yung, "Evaluating the US-China Cybersecurity Agreement, Part 2: China's Take on Cyberspace and Cybersecurity," *The Diplomat*, January 19, 2017, http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity/

a. Genuine Attempt at Cooperation

In the year since the Agreement, some analysts have claimed the results represent a genuine attempt at cooperation. Scott Warren Harold, associate director of the *RAND Center for Asia Pacific Policy,* claims the Agreement is "a good first step."[36] He explains, similar to President Obama, that the Agreement is progress towards addressing the "problem of Chinese espionage."[37] Prior to the Agreement, the United States has been essentially hemorrhaging money for years due to the EMCE and has faced numerous intrusions, but since the Agreement has seen a reduction of intrusions of U.S. companies from China. He elaborates that "a genuine reduction in Chinese economically-motivated cyber espionage could go some way toward easing tensions in the broader bilateral U.S.-China relationship."[38]*FireEye's* report, "Redline Drawn: China Recalculates its use of Cyber Espionage," also suggests a drop in attacks following the Agreement after an analysis of attacks by "suspected China-based groups" from February 2013 to May 2016.[39]

b. No Major Impact

The dominant opinion, including *FireEye*, however, is that the Agreement has made no major impact. Rather than seeing the Agreement as a "watershed moment," critics, instead, argue the Agreement is "one point amongst dramatic changes that had been taking place for years."[40] The U.S.-China Economic and Security Review Commission (USCC) provide a good summary of this perspective in the "2016 Annual Report to Congress."[41]

---

[36] Scott Warren Harold, "The US-China Cyber Agreement: A Good First Step," *The Cipher Brief,* July 31, 2016, https://www.thecipherbrief.com/article/tech/us-china-cyber-agreement-possibly-good-first-step-1092.

[37] Harold, "The US-China Cyber Agreement"

[38] Ibid.

[39] FireEye, "Redline Drawn: China Recalculates its use of Cyber Espionage" (special report, FireEye, June 2016), https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

[40] Ibid.

[41] U.S.-China Economic and Security Review Commission, "2016 Annual Report to Congress," November 2016, http://www.uscc.gov/annual_report/2010/Chapter3_Section_1%28page119%29.pdf.

The USCC authors point out, public reports from *FireEye* and *CSIS* are unable to attribute the decline in frequency of attacks to the Agreement.[42] Instead, punitive measures by the United States against China better explains the data as seen in a graph by Matt Tait, founder of *Capital Alpha Security,* displayed in Figure 1.[43]

[42] Ibid.

[43] Matt Tait, Twitter post, 21 June 2016, 11:43 a.m., https://twitter.com/pwnallthethings/status/745280882076958720.

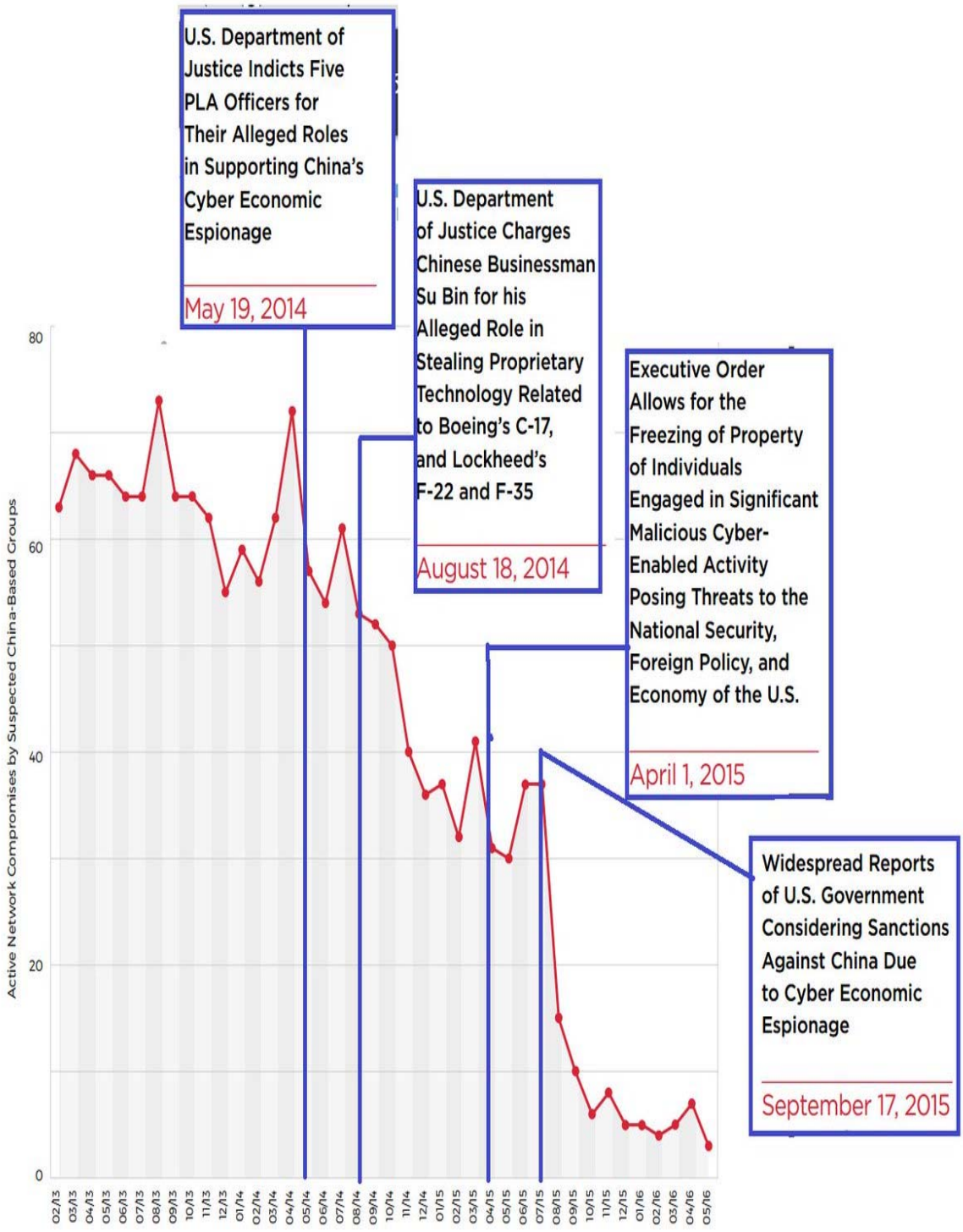


Figure 1. FireEye's Data Overlaid with Policy.[44]

[44] Matt Tait, Twitter post, 21 June 2016, 11:43 a.m., https://twitter.com/pwnallthethings/status/745280882076958720.

It appears that punitive measures, rather than the Agreement, have caused the decline (Figure 1). The decline begins in 2014, before the Agreement, and continues. The major inflection points coincide with punitive actions taken by the United States against China. Provided this data, the view of the proverbial stick as the necessary element, a view that Dmitri Alperovitch, co-founder of CrowdStrike, has argued for years as necessity to "deter Chinese economic espionage against U.S. companies," seems reasonable.[45]

c. Feigned Cooperation

Alternatively, while evidence suggests a drop in the volume of attacks, analysts debate whether volume is even the right metric to use. The overall drop in attacks could also represent a shift from "prolific amateur attacks toward more centralized, professionalized, and sophisticated attacks by a smaller number of actors."[46] In a 2015 hearing before the USCC, Mr. John Costello, Congressional Innovation Fellow, New America, explained that the threat of Chinese theft and espionage has not gone down but instead changed to that of a "Russian model."[47] He explains that China's model faced several problems operating in cyberspace because of their decentralized model of control.[48] Their cyber actors struggled at deconflicting efforts; multiple actors attacked the same target, repeating efforts. Thus, the drop in attacks could instead represent the adoption of a more sophisticated and centralized model (i.e., the Russia Model). A Congressional Research Report on the Chinese Military provides support evidence as China appears to focus on modernizing their military towards "quality over quantity."[49]

---

[45] Dmitri Alperovitch, "U.S. – China Agreement on Cyber Intrusions: An Inflection Point," *Crowdstrike (*blog), September 25, 2015, https://www.crowdstrike.com/blog/cyber-agreement/.

[46] U.S.-China Economic and Security Review Commission, "2016 Annual Report to Congress."

[47] U.S.-China Economic and Security Review Commission, "Hearing Before the U.S.-China Economic and Security Review Commission," June 09, 2016, https://www.uscc.gov/sites/default/files/transcripts/June%2009,%202016%20Hearing%20Transcript.pdf.

[48] Ibid.

[49] Ian E. Rinehart, "The Chinese Military: Overview and Issues for Congress," (CRS Report No. R44196) (Washington, DC: Congressional Research Service, 2016), https://fas.org/sgp/crs/row/R44196.pdf.

Similarly, rather than cooperation, the Agreement could also be a tool in China's changing military strategy. As Harold, Libicki, and Cevallos explain, China might use the Agreement to provide the CCP with the authority to "rein in its own freelance hackers."[50] Breaking hackers into two basic groups of amateurs or elites, China has elite teams like APT1 and amateur groups like freelance or moonlighting hackers.[51] The Agreement can provide the CCP with an excuse to stop attacks outside of the CCP's purview by leveraging the United States as the oppressor forcing China's hand.

The common theme in each explanation is that so far the Agreement has had little to no impact. Either the Agreement simply happened while punitive actions were already creating a decline, or the Agreement is a tool that enhances China's strategy. In any case, these views present a picture of little to no promise of an international agreement working to solve the issue of cyberespionage and theft.

This pessimistic diagnosis, however, is based on casual use of evidence and is still far from a forgone conclusion. Hence, this thesis examines the Agreement in two ways. First, current evidence is lacking in two ways: one, the data used only explores attacks up to May 2016, a relatively short time frame; and two, it uses volume as the sole metric. As a result, this thesis research provides updated data and analysis of a full year of data since the Agreement; and this thesis measures attacks using alternative measurement criteria. Second, this thesis expands current views to include broader implications of the Agreement including impacts to U.S.–China relations and the development of global cyber norms.

3. Potential Areas to Measure

While much of the commentary presents a pessimistic view and suggests little impact from the Agreement, the only metric the articles refer to is the volume of cyberattacks, which begs a broader question. How can the United States measure success of the Agreement?

---

[50] Harold, Libicki, and Cevallos, *Getting to Yes with China in Cyberspace*.

[51] Nigel Inkster, China's Cyber Power (Abingdon: Routledge ; London : The International Institute for Strategic Studies, 2016).

a. Costs of Cybercrime

At a broader level, researchers have utilized economic impact as a measurement of cybercrime and espionage. In a 2015 report to Congress, the U.S.-China Economic and Security Review Commission (USCC) used a cost estimate from McAfee's cybersecurity branch of "$375 billion to $575 billion annually worldwide."[52] Lloyd's Risk Index provides a similar figure of "$400 billion a year."[53] Neither, however, compares to the estimate provided by Cybersecurity Ventures, $3 trillion in 2015.[54] The range indicates a high amount of variance, the reciprocal of precision. The reason why is simple: each group has a different way to calculate the costs.

Moreover, even though Lloyd and McAfee both identify similar numbers, their methodology of calculation is different. In Lloyd's calculation, their figure is formulated by accounting for "restitution, fines, business disruption, legal and remediation services."[55] Lloyd's calculation focuses on direct costs to business, costs that are relatively easier to identify because they are actual and realized by business. McAfee, on the other hand, includes indirect costs into their calculation, which includes items like "additional costs for securing networks, and the cost of recovering from cyberattacks, including reputational damage to the hacked company."[56] Indirect costs, as McAfee emphasizes, "show the full effect of cybercrime."[57] Comparing McAfee and Lloyd's estimates, however, does not appear to support McAfee's argument of indirect costs. If indirect costs were a more significant factor, McAfee's estimate should be significantly

---

[52] U.S.-China Economic and Security Review Commission, "2015 Annual Report to Congress," November 2015, http://origin.www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF, 515.

[53] Francesca Spidalieri, *Understanding Cyber Threats: Lessons for the Boardroom,* report, September 2016, accessed February 15, 2017, http://pellcenter.org/wp-content/uploads/2016/09/Understanding-Cyber-Threats-Lessons-for-the-Boardroom.pdf.

[54] Morgan, *Hackerpocalyse*.

[55] Spidalieri, *Understanding Cyber Threats.*

[56] McAfee, *Net Losses.*

[57] Matthew Benigni, Kathleen M. Carley, and Sumeet Kumar, "The Impact of U.S. Cyber Policies on Cyber-Attacks Trend," *Carnegie Mellon University,* http://www.casos.cs.cmu.edu/publications/papers/2016ImpactofUSCyber.pdf.

higher than Lloyd's. Rather than definitive proof of economic damages, the three different calculations show the difficulty in trying to estimate a specific figure.

b. Cyber Policies as Measurement Criteria

Other methods have also measured the impact of the Agreement. Similar to Tait, in the article "The Impact of U.S. Cyber Policies on Cyber-Attacks Trend," the authors challenged presumptions that cyberattacks on the United States are increasing.[58] Within their methodology, they perform a trend analysis comparing the different year's data against each other. Then, the authors, similar to Tait, attempt to find specific policies to compare against the data and discover whether there is correlation. Their analysis, however, found little statistical evidence of the Agreement causing any significant changes. Although comparing policy actions against trends in cyberattacks provides some room to provide a better picture of the policy impacts following the Agreement, current results have yet to produce promising results.

This thesis will advance the use of cyber policies as a measurement criterion by providing a comprehensive summary and analysis of China's cyber policies. By detailing cyber policies from before and after the Agreement, this thesis examines the changes China has, or has not, made. Then, utilizing changes in policy as a measurement criterion, a trend analysis will highlight the degree to which the Agreement has made an impact.

4. Broader Impacts

Also missing from current assessments of the Agreement is an analysis of the broader impacts, any impacts beyond the four main stipulations, listed below (full text in Appendix A), in the Agreement:

1. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory.
2. Neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property.

[58] Ibid.

3. Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community.
4. The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues.[59]

At the immediate onset of the Agreement, analysts like Adam Segal speculated the Agreement could affect much more than just the flow of cyberattacks and espionage.[60] They suggest that the Agreement, borrowing the influences from the United States and China, could send a global message signifying major changes to international institutions and norms. Indeed, since the signing, scholars have noted some signs of broader impacts.

One impact the Agreement seems to have made is propagating more bilateral agreements. As Segal discussed, "a month after signing the agreement with the United States, China inked a similar deal with the United Kingdom, and, in November 2015, China, Brazil, Russia, the United States, and other members of the Group of Twenty accepted the norm against conducting cyber-enabled theft of intellectual property."[61] With more countries forming bilateral agreements pledging that state sponsored cyber espionage is unacceptable, norms against cyber espionage begin to form.

Evaluation of institutions and norms emerging because of the Agreement, however, has yet to be undertaken beyond informal speculation.[62] A review of institutions, laws, or regulations before and after the Agreement could lead to a much different evaluation than current commentary. If little has changed, the arguments presented by current skeptics would hold more weight, and thus, like some analysts suggested, policy should focus on punitive measures to ensure results. If, however, the

---

[59] "FACT SHEET: President Xi Jinping's State Visit to the United States."

[60] Joseph Marks, "Obama, Xi vow not to steal each others' secrets," Politico, September 25, 2015, accessed March 11, 2017, http://www.politico.com/story/2015/09/obama-xi-vow-not-to-steal-each-others-secrets-214077.

[61] Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later," Council on Foreign Relations, September 28, 2016, accessed March 21, 2017, http://blogs.cfr.org/cyber/2016/09/28/the-u-s-china-cyber-espionage-deal-one-year-later/.

[62] Gary Brown and Christopher D. Yung, "Evaluating the US-China Cybersecurity Agreement, Part 3," *The Diplomat*, January 21, 2017, accessed March 21, 2017, http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/.

trend of institutions suggests true cooperative efforts, the results of the Agreement may be more than just a good first step. Put more simply, as Doug Olenick considers, is the Agreement like the "Treaty of Versailles" or "the Strategic Arms Limitation Talks (SALT)?"[63] The Treaty of Versailles failed, while SALT, arguably, impacted much more than just the United States and the Soviet Union. The Agreement could fall into either path, or somewhere between, but the results need exploring to evaluate which is more likely or evident so that the United States can better focus strategic efforts to prevent or lessen cyber theft.

D. POTENTIAL EXPLANATION AND HYPOTHESIS

Building on a broader base of evidence of the actions taken since Agreement, this thesis examines two principal variables: whether the Agreement generated generally positive or negative results, and whether or not it has had impact beyond its explicit objectives. These variables yield four possible predictions for emerging conditions (Figure 2).

[63] Doug Olenick, "U.S.-China Cyber Agreement: Flawed, but a step in the right direction," SC Media, January 24, 2017, accessed March 11, 2017, https://www.scmagazine.com/us-china-cyber-agreement-flawed-but-a-step-in-the-right-direction/article/633533/.

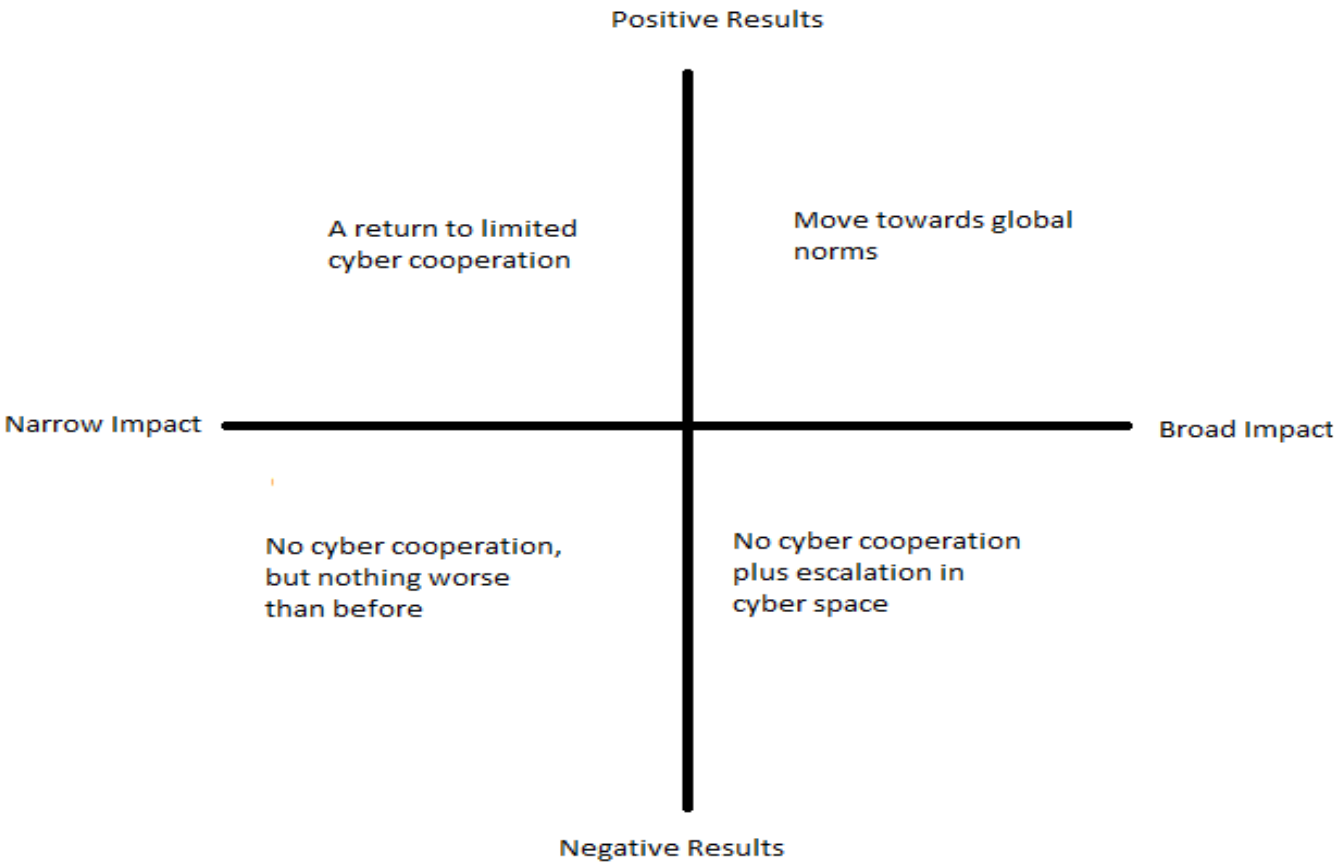


Figure 2. Potential Outcomes

1. Variables

On the X-axis, the endpoints are defined by whether or not the Agreement has created or is creating broader impacts. A narrow impact implies the results are limited to the specific stipulations outlined in the Agreement, essentially affecting only state sponsored espionage and not much more. The two sides, then, likely are not seeking expansive roles or importance in creating global cyber norms. Conversely, a broad impact means the results expand beyond the scope of the Agreement and play a larger role, influencing changes in either domestic or international institutions.

On the Y-axis, the endpoints are defined by the results of the Agreement. On one end, positive results refer to a decrease in attacks by volume or by the criteria of more qualitative analysis based on policy and institutionalization impacts. Negative results are trends toward the opposite, an increase in volume and/or severity of attacks, and little to no policy or institutional changes.

2. Prospects

Based on the disposition of these variables, four possible general directions for future developments are possible. The time period since the Agreement is rather short, and too many other factors are involved, to make reliable predictions for future developments. However, appreciating these general tendencies will allow the thesis, in its conclusion, to examine policy-relevant implications of its findings.

E. RESEARCH DESIGN

This thesis will focus primarily on determining the current circumstances for each axis. To determine the Y-axis, an analysis of attacks will be performed using two metrics. First, given another year since FireEye's data, this thesis will revisit data on the volume attacks. By synthesizing data from FireEye as well as Statista and Hackmageddon, this thesis provides a more thorough evaluation of the statistical data.

Second, this thesis repurposes the Schmitt Analysis to help determine whether the results of the Agreement are positive or negative.[64] The Schmitt Analysis, originally designed as a legal framework for casus belli, provides an alternative to measuring cyberattacks rather than assessing attacks only by volume or by technique. Professor Schmitt suggested a framework of seven "factors that would likely influence assessments by States as to whether particular cyber operations amounted to a use of force."[65] This thesis will adapt the Schmitt Analysis to provide a common and more expansive measurement to distinguish significant from incidental cyberattacks. Applying this measure of time can provide a more accurate litmus test of whether China's behavior in cyberspace has changed. Using the seven Schmitt Analysis criteria may reveal trends in Chinese cyberattacks that continue to cross different thresholds or show a more positive trend with a decline of cyber brinksmanship. Moreover, the seven different factors help overcome a reliance on only measuring volume of attacks and the pitfalls of using singular variable framework.

This application is an expansion of prior similar applications of the Schmitt Analysis. In the paper, "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System," the authors add a quantitative scale to each of the factors. By applying a numeric rating, the authors attempt to narrow the "'grey area' of uncertainty" and provide "a framework for evaluating differences in interpretations of the law."[66] This thesis utilizes the same quantitative scale to provide a "more academically rigorous evaluation."[67] By applying a stable metric via use of the Schmitt Analysis, this thesis may provide a better determination of whether attacks are more sophisticated or severe than previously.

---

64 Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, (Washington, DC: National Academies Press, 2010), 151–177.

65 Ibid.

66 James B. Michael, Thomas C. Wingfield, and Duminda Wijesekera, "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System," in *Proc. of 27th Annual International Computer Software and Applications Conference*, pp. 622–626, November 3–6, 2003.

67 Michael, "Measured Responses to Cyber Attacks Using Schmitt Analysis."

Lastly, this thesis will research and compile China's cyber policies prior to and after the Agreement. Then, taking the analysis of volume of attacks and Schmitt Analysis, a comparison of both will be made against China's cyber policies to help confirm or eliminate policy impacts as a causal element as Tait had done previously.

To determine the X-axis, this thesis looks at institutional changes domestically and internationally. First, again taking a look at China's policies, this thesis analyzes changes over time to identify whether or not the Agreement has made broad impacts. If the changes are limited to the stipulations in the Agreement, the impact from the Agreement is narrow. If, however, Chinese policies aim at changing behavior further than just the stipulations, then the impact is broad. Second, this thesis examines other agreements made internationally that contain elements similar to Agreement. Propagation of similar cyber norms implies a broader impact resulting from the Agreement.

F. THESIS OVERVIEW AND CHAPTER OUTLINE

In order to explore impacts of the Agreement, this thesis is divided into five chapters. Chapter II begins by broadening the analytical scope, looking at policies to determine whether cooperation has expanded beyond the Agreement in terms of either U.S.–China relations or broader global cyber activities. Chapter III then reexamines FireEye's data and making a deeper inspection on the volume of cyberattacks. Chapter IV explores an alternative method of measuring cyberattacks, the Schmitt Analysis. Finally, Chapter V summarizes the findings, discusses policy-relevant implications and gives recommendations for further research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE U.S.-CHINA CYBER AGREEMENT AND CHINESE CYBER POLICY[68]

A. INTRODUCTION

In the two years following the Agreement, few articles discuss Chinese compliance to their commitment outside the sheer volume of cyberattacks. Analysts generally focus on the volume of cyberattacks as the sole criteria in which to measure the results of the Agreement. As a result, the United States needs to expand analysis of the Agreement. Has the Agreement or effects of the Agreement resulted in broader impacts to Chinese cyber policies? This chapter explains that the actions taken by the Chinese government suggest the Agreement represents a sincere effort to honor the spirit of cyber-cooperation.

Over the past two years, major changes in Chinese cyber policies and other related areas suggest that the Agreement influenced Chinese behavior outside of the specific stipulations. From the formation of new cyber laws and bilateral agreements to different language used in political rhetoric, the PRC's position appears to be changing, which raises key questions. How much has and/or is the PRC's cyber position changing and in what direction? This chapter attempts to answer both questions by analyzing China's official and unofficial cyber policies and the U.S.-China relationship pre- and post-Agreement. It first revisits the terms and define the specific parameters of the Agreement. Then, it explores the pre- and post-Agreement eras, respectively. Last, it explains the findings and provides an interpretation of the data.

This review in this chapter finds a discernable change in Chinese policies from the pre- to post-Agreement periods. During the pre-Agreement period, the PRC gave little focus and attention to official cyber policies, generally lacking any cybersecurity laws. Instead, the PRC's cyber doctrine relied on an unofficial doctrine, showing a consistent effort by Chinese actors to engage in cyber theft and espionage. Additionally, the PRC's efforts to engage in U.S.-China cyber relations seemed insincere bilateral talks failed to

[68]Chapter II of this thesis was used as the final paper for NS4642 (Summer 2017) with Dr. Glosny.

generate changes in China such as formal or informal cooperation between U.S. and Chinese law enforcement agencies. In the post-Agreement period, however, concerted efforts by the CCP suggest a drastically different position. New cybersecurity laws and strategies show greater government involvement to regulate and manage cyberspace. Formal information sharing and cooperative mechanisms between U.S. and Chinese law enforcement that include exchanging phone numbers also suggest change at different levels including the bureaucratic level. In the end, the Agreement not only changed the volume of attacks, but also Chinese policies and governance of cyberspace.

B. THE 2015 AGREEMENT

In general, the United States and China reaching an agreement is a major historical moment. While not permanently binding, the language and specific stipulations in any agreement play major roles in shaping both countries' relationship with each other as well as other nations. The formation of the 2015 U.S.-China Cyber Agreement will likely be no exception, but, as seen in previous agreements, the question is to what degree. As a result, defining what exactly each side agreed to is paramount to understanding how much of an impact the Agreement has made. Take, for example, the case of the 1982 Communique, where the CCP has criticized and still criticizes the United States for failing to uphold promises to reduce weapon sales to Taiwan. The impact was fairly narrow as U.S. promises did not expand to include military technology as well as other items. The United States must, then, identify the stipulations of the Agreement and defines what would constitute a broad versus narrow impact.

1. Terms of the Agreement

The terms and stipulations of the Agreement have never been made into a formal document. Instead, the terms were explained through three press releases following the 2015 security summit between President Obama and President Xi. They presented the initial release in a joint press conference by the two presidents on September 25, 2015, which was later provided as a transcript by the U.S. Office of the Press Secretary. The second release, also from the U.S. Office of the Press Secretary, came in the form of a fact sheet that summarized the views exchanged between the two presidents. Last, the

Ministry of Foreign Affairs of the People's Republic of China (FMPRC) also released a summary of outcomes from the summit. Appendix D provides the specific language from the three documents concerning the Agreement.

Although both sides emphasize different items, there are several areas of overlap from which this thesis can derive the exact stipulations of the Agreement. In particular, nearly identical language can be seen in the White House's "Fact Sheet" and the FMPRC's "Outcome list."[69] Focusing on the overlapping language, the stipulations covered under the Agreement can be identified as the following:

- Neither state will "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage, with the intent of providing competitive advantages to companies or commercial sectors"[70]
- Both states will work with other nations to promote and establish international rules and norms of conduct in cyberspace[71]
- Both states will jointly fight cybercrime, including investigation assistance and information sharing[72]
- Both states will establish a "high-level joint dialogue mechanism to fight cybercrime and related issues," including:[73]
  - Establishment of a cyber hot-line
  - Mechanism to review timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity identified by either side
  - Minimum of two dialogue meetings per year

Superficially, the terms of the Agreement are fairly straightforward. Both President Obama and President Xi identified an alarming trend moving their countries toward conflict and, as a result, cooperated to avoid entering a Prisoner's Dilemma.

69 "FACT SHEET: President Xi Jinping's State Visit to the United States"; "Full Text: Outcome list of President Xi Jinping's state visit to the United States."

70 "Full Text: Outcome list of President Xi Jinping's state visit to the United States."

71 Ibid.

72 "First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes."

73 "Full Text: Outcome list of President Xi Jinping's state visit to the United States."

Furthermore, both sides agree that the problem is not just one between the United States and China but a global problem with far-reaching implications. Therefore, the two sides agree that, as the largest cyber power and largest cyber user base, respectively, the United States and China must lead the change in global cyber behavior. More notably, the two separate fact sheets released by each government contain nearly identical text with the only real difference being that the U.S. version states "the United States and China," whereas the Chinese version states "China and the United States" or "both sides."

A deeper analysis of the terms, however, reveals that there are several ways to interpret compliance. More specifically, since none of the documents explain what compliance would look like, fulfilling the terms can vary greatly. As Wharton professor Marshall W. Meyer points out, implementation of the Agreement will be difficult because the language is "full of ambiguity. What's the line between government and business? Also, especially in China, which government are we talking about?"[74] These questions, among many others, highlight the importance of how each country interprets actual compliance, which, as a result, will vary the possible scale and scope of cooperation. Therefore, as a reflection of Chinese intentions, the focus must be on Chinese actions.

2. Broad versus Narrow Impact

Depending on Chinese actions, the results following the Agreement will either be broad or narrow, thus helping to determine Chinese intentions. Broader impacts are actions taken beyond the specific interpretations of the terms and narrow impacts are much more limited actions. For example, while both sides agree to jointly fight cybercrime, a narrow interpretation does not mean actual cooperation must occur as the Agreement does not specify or name which agencies will cooperate nor does it dictate what "government" must make any policy changes domestically.[75] Conversely, outcomes suggesting a broader impact would be actions like an arrest of a Chinese citizen by Chinese law enforcement stemming from a U.S. investigation.

---

[74] Jacques deLisle and Jeffrey Vagle, "The Download on the U.S.-China Cyber Espionage Agreement," Wharton, September 30, 2015, http://knowledge.wharton.upenn.edu/article/the-download-on-the-u-s-china-cyber-espionage-agreement/.

[75] Ibid.

Thus, this thesis characterizes actions following the Agreement between two endpoints. In the case of a narrow impact, Chinese actions are limited, following a limited and literal interpretation of each stipulation. Complying with the first stipulation, for instance, actions show little to no change in behavior. Cyberattacks and theft of intellectual property could continue as the terms specify state involvement. Given that the CCP has consistently stated that the government has not played a role in any the cyberattacks they have been accused of, the CCP, then, has nothing to change. Additionally, cooperative efforts under the second through fourth stipulations do not necessitate any actual results. Since international law nor the Agreement include legal mechanisms such as a motion for discovery, China can choose not to share information and the United States cannot prove Chinese agencies did not respond in a timely manner.

At the other end, however, it is possible that the overall results of the Agreement show a much broader impact. Expanding on the first stipulation, for example, the CCP could interpret the definition of "state-sponsored" to include efforts to prevent and punish government involvement rather than just not ordering cyber theft operations.[76] Imaginably, a change in government conduct could include sweeping policy changes like punishment for rogue PLA actors and regulations prohibiting the use of illegally obtained intellectual property. Likewise, cooperative actions could potentially include extradition agreements and/or the formation of an international joint task force akin to ones under Interpol. Consequently, going back to President Obama's point of whether "words are followed by actions," the United States must also ask to what degree.[77]

3. Summary of the Agreement

Overall, however, one can draw a few conclusions from the terms. First, the Agreement makes an attempt at drawing a line concerning the intent behind cyber espionage. President Obama and President Xi each make statements clarifying that cyber espionage for industrial/commercial theft is distinctly different from using cyber

[76] deLisle and Vagle, "The Download on the U.S.-China Cyber Espionage Agreement."

[77] "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference."

espionage to support national security and/or other interests. Secondly, while neither side specifically states any punishment for violating these stipulations, they make a point to highlight the consequences if the two cease cooperative efforts. In particular, statements by President Xi succinctly point out "confrontation and friction are not made by choice for both sides," emphasizing the idea that the two sides are trapped in a Prisoner's dilemma with a negative end result that "confrontation will lead to losses on both sides."[78] Lastly, the ambiguity in the language of the text provides opportunities by either side to shape the scale and scope of the Agreement. The purpose of a cyberattack can often have multiple interpretations, particularly for dual-use technologies, and with loose standards of timeliness and quality of responses to malicious cyber activity, each side has ample ability to control how much cooperation will take place. In this sense, ambiguity provides an upside flexibility as circumstances evolve. Given the potential consequences, there is ample incentive to go beyond the minimal effort to uphold the Agreement.

C. PRE-AGREEMENT ERA

Prior to the Agreement, China's cyber policy was not well defined as the CCP did not consider cyber policy as a separate entity. Instead, policies were developed as part of an overall "path to informatization" and as part of an overarching security policy.[79] As a result, defining China's cyber policy is complicated, requiring a holistic approach to comprehend. Thus, Section C and D, cover an array of documents and actions that provide context and help define China's cyber policy.

Section C is organized as follows. Part 1 examines official Chinese documents, revealing how the CCP perceived cybersecurity issues and policies. Next, Part 2 discusses unofficial policy. As actions often speak louder than words, repeated incidents of cyber theft suggest China has an unofficial cyber policy that includes strategies such as espionage. Last, Part 3 details the U.S.-China relationship on cyberspace, providing an overview of cooperative and uncooperative efforts.

---

78 "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference."

79 Weizhi Qu, *Chinas Path to Informatization* (Singapore: Cengage Learning Asia, 2010).

1. China's Official Cyber Policies

As described in a 2016 thesis by Vaughn Rogers, China's cyber policy was primarily derived from two sources.[80] The first source is the Information Office of the State Council of the People's Republic of China (SCIO). As part of the PRC's State Council, the SCIO is tasked with disseminating "policies formulated by the Communist Party and laws passed by the National People's Congress."[81] To support that goal, the SCIO releases White Papers which provide a description of both the official policy and overall purpose. The second source is *The Constitution of the People's Republic of China.*[82] Like any other country, China's Constitution defines the underpinnings and purpose of the PRC. As the primary sources for Chinese cyber policy, they were crucial for "how the Chinese government views the Internet and Internet use."[83] From these documents, one can draw a few conclusions.

The Internet and its development, from China's perspective, were paramount for China's growth. As described in the 2010 White Paper, "The Internet in China," demand for information would only continue to grow, thus the government must strived to provide people with access.[84] Policy, therefore, focused on four items: "active use, scientific development, law-based administration and ensured security."[85] To that effort, from 1997–2009, the PRC invested "4.3 trillion yuan" into cyber infrastructure, which eventually led China to contain the largest number of Internet users in the world.[86] Even so, the PRC recognizes there was still a disparity between urban and rural users as a

---

[80] Vaughn C. Rogers, "The History of Chinese Cybersecurity: Current Effects on Chinese Society Economy, and Foreign Relations" (master's thesis, Seton Hall Univeristy, 2016) http://scholarship.shu.edu/dissertations/2207.

[81] Susan V. Lawrence, China's Political Institutions and Leaders in Charts (CRS Report No. R43303) (Washington, DC: Congressional Research Service, 2015), https://fas.org/sgp/crs/row/R43303.pdf.

[82] "Constitution of the People's Republic of China," People's Daily Online, accessed August 24, 2017, http://en.people.cn/constitution/constitution.html.

[83] Rogers, "The History of Chinese Cybersecurity," 13.

[84] Information Office of the State Council of the People's Republic of China, "The Internet in China," China.org.cn, accessed August 24, 2017, http://www.china.org.cn/government/whitepaper/node_7093508.htm.

[85] Information Office of the State Council of the People's Republic of China, "The Internet in China."

[86] Ibid.

result of imbalanced development, driving the PRC to focus on development. Overall, however, the recurring theme was a push toward growth and the Internet as an enabling pillar to that goal.

While cyberspace as the pillar for growth was the primary goal, the PRC also recognized that addressing security threats was quickly becoming a goal of equal importance. In 2015, the White Paper, "China's Military Strategy," the SCIO explained China faces a crisis as both a competitor in an "international security competition" and as "one of the major victims of hacker attacks."[87] While the statement was likely a response to previous U.S. accusations including the 2015 indictment of five PLA Officers, previous documents showed consistent opposition to cyberattacks. The 2010 paper claimed that of the all the computers infected by the "Conficker virus," China accounted for around 30% of the total.[88] Thus, even much earlier than the Agreement, China's official position has consistently been against cyberattacks.

Furthermore, China also consistently maintained a policy of pursing development peacefully and to make a concerted effort toward international cooperation. Both in China's Constitution and in the 2011 White Paper, "China's Peaceful Development," the PRC reiterated that China must "live up to international responsibility" and respect "others' security concerns."[89] Hence, China's cyber policy should be promising.

Overall, PRC goals, in principle, matched the United States. The Internet is of the utmost importance. The government is charged with providing access and security to the public, while ensuring actions remain peaceful. Why, then, did so many cyberattacks occur? The problem was China's unofficial policy and glaring holes in official policy.

---

87 "Full text: China's Military Strategy," China Daily, last updated May 26, 2015, accessed August 25, 2017, http://www.chinadaily.com.cn/china/2015-05/26/content_20820628_4.htm.

88 Ibid.

89 "China's Foreign Policies for Pursuing Peaceful Development," China.org.cn, accessed August 25, 2017, http://www.china.org.cn/government/whitepaper/2011-09/06/content_23362744.htm.

2. China's Unofficial Policies

As detailed in several reports including official testimonies to the U.S. Congress, the reality has been that the Chinese government uses cyber espionage as an immensely effectively tool.[90] One estimate in 2015 claimed China was "responsible for as much as 80% of all intellectual property theft against U.S. companies."[91] Although many other reports, such as Akamai, showed significantly lower figures, China was consistently one of the largest perpetrators of cyberattacks.[92] Even discounting information warfare operations between the United States and China, there was an apparent disconnect between official policy and reality. CCP policy may not have directly dictated or advocated cyberattacks, but, for the United States at least, attacks were the expectation. From the 2003 intrusion of DOD systems by *Titan Rain* to *Operation Aurora* in 2010 to the 2015 attack on the Office of Personnel Management (OPM), there appeared to be a consistent effort by Chinese actors to steal and spy from the United States.[93]

Moreover, behind these efforts, there appeared to be an unofficial doctrine of how the Chinese operate. Similar to a corporate business plan, Chinese actions displayed a complete logistics cycle of "acquisition, absorption, and application."[94] As shown in Figure 3, there was, to some degree, a doctrinal model of operations.

---

[90] U.S.-China Economic and Security Review Commission, "China's Intelligence Services And Espionage Operations," June 9, 2016, https://www.uscc.gov/sites/default/files/transcripts/June%2009%2C%202016%20Hearing%20Transcript.pdf.

[91] Ibid., 69.

[92] Ibid.

[93] Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity* (New York: 2015), edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron: 51–86.

[94] Lindsay and Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application."

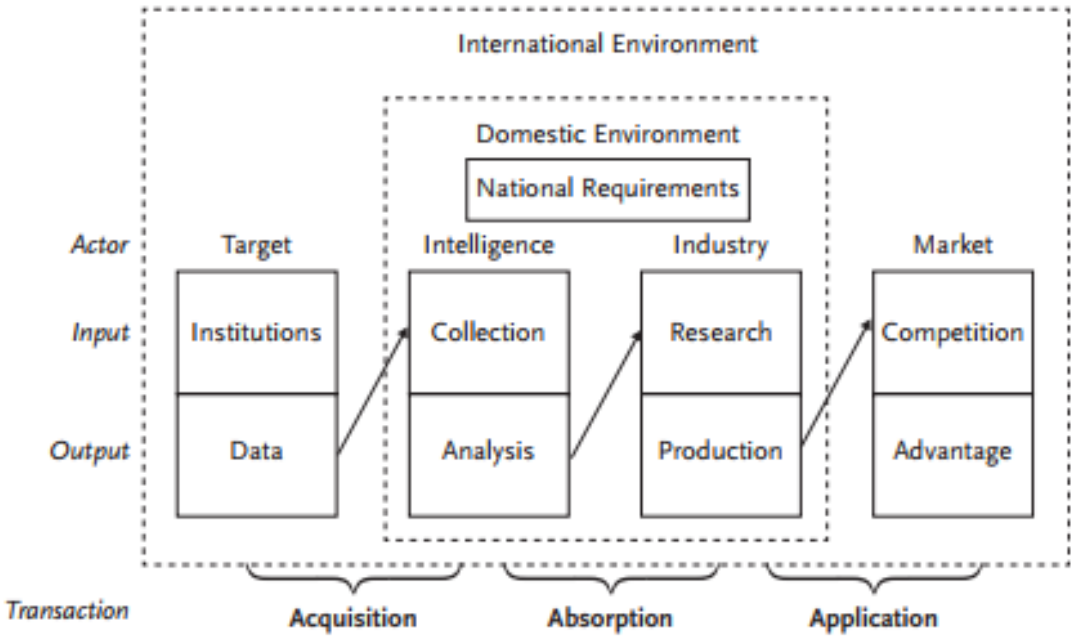


Figure 3. A Model of Espionage Effectiveness[95]

While the model in Figure 3 is far from a detailed layout of operations, analysts have identified enough of a pattern in Chinese actions to frame a pseudo-doctrine of operations. More specifically, the authors of *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* dispelled several myths and provided details of Chinese industrial espionage.[96] For example, in terms of acquisitions, analysts found widespread evidence of CCP programs that include "the use of open source, foreign R&D in China, PRC-based transfer organizations, U.S.-based facilitators, the role of overseas students and scholars, PRC policy initiatives, clandestine support for technology transfer, and China's abuse of cyber space."[97] Moreover, evidence of these programs included empirical proof such as discovering that "Larry Wu-Tai Chin was paid 'about a million

[95] Lindsay and Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application."

[96] Ibid.

[97] William Hannas, Anna B. Puglisi, and James C. Mulvenon, *Chinese Industrial Espionage: Technology Acquisition And Military Modernisation* (London: Routledge, 2013), 230.

dollars' by Chinese intelligence."[98] Overall, there is an identifiable process that can basically be called policy.

Even accepting that not all of the actors were directly tied to the state, many of the non-state actors were such that they are better described as "'partial state actors."[99] China utilized the complexity and relative uncertainty of attribution as a form of plausible deniability, but if one asks "'cui bono?', it is hard to reach any other conclusion than that their perpetrators were acting in the perceived interests of Beijing."[100] Much of the data stolen had little use for the private sector. Military technology, and OPM data, among other things, were not in much demand. Thus, following the laws of supply and demand, there must have been some level of demand for the market to function; actors must be incentivized to steal information. Assuming, of course, a rational actor model, either there was enough nationalism for the propagation of patriot actors or, perhaps more likely, some sort of compensation offered by the Chinese government such as potential employment or a monetary exchange. In either case, the CCP, directly or indirectly, seemed to have a policy that enables a market for cyber espionage.

3. U.S.–China Relations in Cyberspace

China's official and unofficial policies complicated the U.S.-China relationship. Official policies stated that a rivalry is debilitating and, therefore, required a level of cooperative effort. As a result, in February 2012, President Xi and President Obama agreed to forge a "cooperative partnership."[101] Unofficially, however, Chinese actions seemed to test U.S. boundaries of what can be proven. Thus, against a backdrop of accusations and mistrust, from 2012 up until the Agreement, U.S.-China relations in cyberspace seemed insincere.

---

[98] Hannas, Puglisi, and Mulvenon, *Chinese Industrial Espionage*, 194.

[99] Nigel Inkster, "Cyber Espionage," in *China's Cyber Power* (Abingdon: London, 2016): 51–82, 67.

[100] Inkster, "Cyber Espionage."

[101] Susan V. Lawrence, U.S.-China Relations: An Overview of Policy Issues (CRS Report No. R41108) (Washington, DC: Congressional Research Service, 2013), https://fas.org/sgp/crs/row/R41108.pdf, 8.

For the most part, China never seemed to take U.S. allegations of "official Chinese actors' involvement in enabled-theft of intellectual property" seriously.[102] Instead, responses were limited to dismissing the allegations or claiming that China faces the same or greater level of attacks. Like most problems, the first step is simply to admit a problem exists, so, from the U.S. perspective, China's unwillingness to admit a problem made it impossible to seek resolution.

Even considering the bilateral groups and talks, words never turned into action. From establishment of a "Cyber Working Group (CWG)" in 2013 to its subsequent suspension in 2014, the two sides agreed to cooperate on issues, but never identified any exact areas of consensus or produced any mechanisms to enhance cooperative efforts.[103] The CWG, as a confidence-building tool, thus, was short-lived and relatively ineffective. Furthermore, 2009–2012 talks between the Cooperation in Cybersecurity China Institute of Contemporary International Relations (CICIR) and Center for Strategic and International Studies (CSIS) identified similar problems.[104] Cooperation between law enforcement agencies is essentially non-existent, and the "U.S. will require some agreement to constrain proxies as part of any larger agreement or CICIR proposed Code of Conduct."[105] Thus, up until the Agreement, there seemed to be little recourse in fixing inherent problems to U.S.-China relations.

D. POST-AGREEMENT

Since the Agreement, cyber policy and cyber-related issues seem to "have grown in importance in relation to China's strategic objectives including its economic, military and political interests."[106] Over the course of two years, the Chinese government made

---

102 Lawrence, U.S.-China Relations, 35.

103 Lawrence, U.S.-China Relations, 35.

104 "Bilateral Discussions on Cooperation in Cybersecurity China Institute of Contemporary International

Relations (CICIR) - Center for Strategic and International Studies (CSIS)," CSIS, June 2012, accessed August 26, 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/120615_JointStatement_CICIR.pdf.

105 Ibid.

106 Caitríona H. Heinl, "New Trends in Chinese Foreign Policy: The Evolving Role of Cyber," *Asian Security* 13, no. 2 (March 2017): 132–147, doi: 10.1080/14799855.2017.1286160.

several new agreements and passed a new cyber law. These developments show that the CCP post-Agreement is different from the CCP pre-Agreement. In sum, while far from definitive proof, China's actions in the post-Agreement era suggest a notable change in CCP's strategic calculus and goals.

1. China's Official Cyber Policies

In contrast to the CCP's pre-Agreement position, it seems that, following the Agreement, the CCP made a concerted effort to change official Chinese cyber policy. Over the last two years, the CCP modernized policies that now separate cyber policy into its own separate and distinct field. Unlike the pre-Agreement era where regulations of cyberspace were a subsidiary of other policies, three major policy developments in post-Agreement China show that this is no longer the case. These developments are as follows: the National Cybersecurity Strategy, the International Cybersecurity Strategy, and the 2016 Cybersecurity Law.[107]

The three developments in Chinese cyber policy are, for the most part, promising for U.S. interests. Collectively, the new policies imply that the CCP intends to be more involved in governing cyberspace and that these intentions are peaceful. With this new role, the CCP appears to be laying out the foundation of cyber policy aligned more closely with U.S. interests in three ways. One, the CCP is beginning to focus on establishing cyber laws and designing law enforcement mechanisms. Two, rather than deflecting responsibility, the CCP is taking an active role in shaping cyber culture. Last, the CCP is also taking further steps to cooperate internationally.

Unlike the pre-Agreement era where cyber laws were relatively ambiguous, post-Agreement China focused on "actual enforcement action."[108] Both the National and International Cybersecurity Strategies iterate the importance and applicability of a "rule-

[107] Samm Sacks, "China's Cybersecurity Law Takes Effect: What to Expect," Lawfare, June 1, 2017, accessed September 1, 2017, https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

[108] Carol A. F. Umhoefer et al., "China: First 100 Days Of Cybersecurity Law Sees Active Enforcement, More Guidelines But Still Uncertainties," *Lexology* (blog), September 4, 2017, https://www.lexology.com/library/detail.aspx?g=fcbcf874-456f-412a-b30c-9b78fe4a3e6b.

based order in cyberspace."[109] Then in conjunction, the 2016 Cybersecurity Law defines exactly what that order looks like and how to comply.[110] For example, the law details network regulations on the collection of personal information as well as potential punishments for non-compliance.[111] In comparison, these rules in pre-Agreement China were non-existent. Thus, one can infer that post-Agreement CCP takes cybersecurity and the regulation of cyberspace, at least to some degree, more seriously. Additionally, in the face of foreign attacks, the government is also responsible for deciding a proper response.[112] Companies and other non-state entities, therefore, do not have free reign to retaliate, but, like similar U.S. counterparts, must rely on the government to make a decision.

Furthermore, the changes in policy infer that the CCP plays a major role in shaping and dictating cyber norms. Domestically, the CCP now states that one of China's strategic tenets must be to strengthen "the construction of online culture."[113] The government, as the CCP argues, needs to guide the Chinese people as to what is moral.[114] As opposed to their earlier stance of a more hands-off approach, the new hands-on tenet marks a shift toward claiming responsibility. Given previous rhetoric that the CCP could hardly be at fault for rogue actors, a proactive effort to shape acceptable behavior in cyberspace is, at a minimum, more promising than reacting dismissively or hoping for a solution with a laissez-faire approach to governance. Even if one accepts the argument that the CCP was always involved with a policy of "e-democracy, i-

---

109 "Full Text: International Strategy of Cooperation on Cyberspace," Xinhua, March 1, 2017, accessed September 4, 2017, http://news.xinhuanet.com/english/china/2017-03/01/c_136094371_4.htm.

110 "Full Text: International Strategy of Cooperation on Cyberspace."

111 Chris Mirasola, "Understanding China's Cybersecurity Law," Lawfare, November 8, 2016, accessed September 4, 2017, https://www.lawfareblog.com/understanding-chinas-cybersecurity-law.

112 Standing Committee of the National People's Congress, "2016 Cybersecurity Law," China Law Translate, November 7, 2016, accessed September 4, 2017, http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en.

113 Roger Creemers, "National Cyberspace Security Strategy," *China Copyright and Media* (blog), December 27, 2016, accessed September 4, 2017, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

114 Ibid.

dictatorship," it was always unofficial.[115] Until the post-Agreement era, there was simply an absence of any official statements and documents focused on how to govern cyberspace. Cyber policy now dictates official responsibility for both creating change and causing it.

The final major area of promise is China's role in cooperating internationally. While labeling pre-Agreement China as uncooperative may be a stretch, there was a notable absence of cooperative efforts internationally with regards to cyberspace. Years of U.S. accusations of cyber theft and espionage seemed to fall on deaf ears. Even discounting China as the perpetrator, one might expect the CCP to show some interests in the Budapest Convention on Cybercrime as China is the "biggest victim of cybercrime."[116] Understandably, Article 32, which involves extraterritorial searches, presents a major concern and a potentially impossible barrier against Chinese interests and ideology, but the CCP neither participated in negotiating the treaty nor pursued an alternative option as they have done in other instances.[117]

Thus, the principles and language under the new policies are somewhat of a surprise, showing a commitment toward cooperative efforts. The International Cybersecurity Strategy states that "international cyberspace governance should feature multi-party participation" to include multiple nations as well as an array of other organizations and that China will "support the international community to consolidate consensus and implement the outcomes."[118] Furthermore, Article 7 under the 2016 Cybersecurity law states that the CCP will participate in "international exchange and cooperation in the areas of cyberspace."[119] The CCP not only signaled to international audiences of its commitment, but also passed official mechanisms in Chinese policy that

---

115 Greg Austin, *Cyber Policy in China* (Cambridge: Polity Press, 2014), 49.

116 Jiang Li, "Commentary: China, biggest victim of cybercrime, champions 'community of common destiny' in cyberspace," Xinhua, December 16, 2015, accessed September 13, 2017, http://news.xinhuanet.com/english/2015-12/16/c_134923452.htm.

117 Qiheng Chen, "Time for ASEAN to Get Serious About Cyber Crime: ASEAN should look to forge its own cyber agreement," *The Diplomat*, August 2, 2017, http://thediplomat.com/2017/08/time-for-asean-to-get-serious-about-cyber-crime/.

118 "Full Text: International Strategy of Cooperation on Cyberspace."

119 Standing Committee of the National People's Congress, "2016 Cybersecurity Law."

help ensure compliance. As a result, official policy seems less about appeasing an international audience and more about actually making changes.

2. Unofficial Policy

Unofficially, the primary question revolves around the reality of Chinese behavior. Do Chinese actions match their words? Although official policy may state that China will cooperate, historically, absence of any effort would suggest that unofficially, China changed very little. If, for example, a cybercriminal is identified and the CCP does nothing to investigate, one can infer that Chinese cyber policy is relatively permissive of such behavior. What this thesis shows, however, is that, to a large extent, Chinese actions comply with not just the terms of the Agreement, but also with the spirit of it. As detailed in Chapters III and IV, there has been a notable decline in cyberattacks. Even outside of cyberattacks, the data indicates a more cooperative and internationally-minded China.

Several arrests over the last two years counter years of complaints that China rarely enforces or punishes malicious actors. In the week following the Agreement, the CCP immediately made a gesture of "good-faith" by arresting an unspecified number of hackers at the behest of the U.S. government.[120] Then in December 2015, perhaps in conjunction with "China's Global Law Enforcement Drive," the United States saw a rare admission from the CCP that Chinese actors "were indeed responsible for compromising the security of the U.S. Office of Personnel Management."[121] Although the admission fell short of admitting state-sponsored activities, the arrest of the five hackers is a concrete start toward proving a commitment toward the Agreement. Additionally, the arrests in 2017 of a criminal operation stealing and selling "private data of Apple users"

---

[120] Ellen Nakashima and Adam Goldman, "In a first, Chinese hackers are arrested at the behest of the U.S. government," *The Washington Post*, October 9, 2015, https://www.washingtonpost.com/world/national-security/in-a-first-chinese-hackers-are-arrested-at-the-behest-of-the-us-government/2015/10/09/0a7b0e46-6778-11e5-8325-a42b5a459b1e_story.html?postshare=9811444395972124&utm_term=.ec6e708bb6cd.

[121] Thomas Eder, Bertram Lang, and Moritz Rudolf, "China's Global Law Enforcement Drive: The Need For A European Response," Mercator Institute for China Studies, January 18, 2017, https://www.merics.org/en/merics-analysis/china-monitor/merics-china-monitor-no-36/#c17722; Andrew Blake, "China Arrests Alleged Opm Hackers, Claims Breach Was Criminal, Not State-Sponsored," *The Washington Times*, December 3, 2015, http://www.washingtontimes.com/news/2015/dec/3/china-reportedly-arrests-alleged-opm-hackers-says-/.

and of the "Fireball" malware developers show a continuous effort to punish malicious actors.[122] While these arrests are far from the 15,000 arrested immediately prior to the Agreement, the pattern falls in line with U.S. expectations that "the proof that the cooperation really is improving" is seeing commitment "sustained over time."[123]

China's pursuit of additional international agreements also suggests the CCP intends to make a continuous, cooperative effort. Currently, the CCP holds similar agreements against conducting "cyber espionage for commercial gain" with "the United States, United Kingdom, Australia, and the G-7 and G-20."[124] Rather than feigning cooperation, China appears to be attempting to establish a global norm against conducting economically motivated cyber espionage. While official policy does not go as far to state such is the goal, signing the myriad of international agreements suggests that is the case for China's cyber policy unofficially.

3. U.S.–China Relations in Cyberspace

In terms of U.S.-China relations, sustained cooperative efforts by the CCP suggest a serious commitment toward "long-term Sino-American relations."[125] From their active participation in high-level working groups during the Obama Administration and recommitment under the Trump administration, the CCP has shown and is showing their cooperative efforts are robust and durable.[126] Whereas the two states only held one

---

[122] Samuel Gibbs, "Criminal Gang Arrested For Selling Apple Users' Private Data In China," The Guardian, June 9, 2017, https://www.theguardian.com/technology/2017/jun/09/apple-employees-arrested-selling-private-user-data-china-criminal; Yi Shu Ng, "China Arrests Hackers Behind One Of The World's Largest Malware Infections," Mashable, July 26, 2017, http://mashable.com/2017/07/26/chinese-hackers-arrested/#_8_MAq3ZSgqn.

[123] Ryan Rifai, "China Says Thousands Arrested For Online Crime," Al Jazeera, August 18, 2018, http://www.aljazeera.com/news/2015/08/china-thousands-arrested-online-crime-150818192622887.html; Nakashima and Goldman, "In a first, Chinese hackers are arrested at the behest of the U.S. government."

[124] Adam Segal, "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?," Council on Foreign Relations (blog), June 29, 2017, https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

[125] Gary Brown and Christopher D. Yung, "Evaluating the US-China Cybersecurity Agreement, Part 3," *The Diplomat*, January 21, 2017, http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/.

[126] Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," Hoover Institution, *Aegis Series Paper*, no. 1703, http://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf, 15.

dialogue during the pre-Agreement era with little result, the U.S. and China not only held three high-level joint dialogues but managed to solidify actual cooperative mechanisms. Highlights of notable mechanisms are as follows:

- Established "guidelines for requesting assistance on cybercrime or other malicious cyber activities and for responding to such requests"[127]
- Conducted a 2016 tabletop exercise on "cybercrime, malicious cyber activity and network protection scenarios to increase mutual understanding regarding their respective authorities, processes and procedures," in which "both sides will assess China's proposal for a seminar on combatting terrorist misuse of technology and communications."[128]
- Established a hotline between the U.S. and Chinese presidents "for escalation of issues that may arise in the course of responding to cybercrime and other malicious cyber activities"[129]
- Established regular meetings at the "ministerial level" to discuss network security[130]
- Designed the mechanism of the "Status Report on U.S./China Cybercrime Cases"[131]
- Formed the "first U.S.-China Senior Experts Group on International Norms in Cyberspace and Related Issues"[132]

As shown, the working groups went above and beyond the specific terms of the Agreement, and have strengthened U.S.-China relations. Each of the mechanisms work as confidence building measures by finding areas of consensus and binding the two sides toward cooperation.

---

127 "First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes," U.S. Department of Justice, December 2, 2015, https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0.

128 Ibid.

129 Ibid.

130 "Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue," U.S. Department of Justice, June 14, 2016, https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue.

131 " Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues," U.S. Department of Justice, December 8, 2016, https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues.

132 "Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue."

Although critics that might argue words still mean little without action, both sides executed their promises. In addition to the arrests and cooperative takedown of "some botnets and fake websites," the two established a more efficient streamline of communication with "a point of contact and a designated email address."[133] Also, on May 11, 2016, the U.S. and China discussed international norms.[134] While results are unclear, the group called the talks "positive, in-depth and constructive."[135] For the most part, actions are following words. The actions are perhaps slow for some and too little for others, but progressive nonetheless.[136]

E. CONCLUSION

The Agreement called only for each state not to engage in espionage for commercial economic gain and for the two sides to attempt to cooperate, but China has done more than that. The CCP made official legal changes. They passed the first comprehensive cyber law in Chinese history, the first national cybersecurity strategy, and the first international cybersecurity strategy. Furthermore, the CCP actually executed many of their promises. From continued meetings to actual arrests, the CCP is holding up its end of the bargain. Thus, from pre- to post-Agreement, there is a discernable, positive change in Chinese cyber policy. Moreover, Chinese cyber policies are more cooperative and more aligned with U.S. interests.

Thus, U.S.-China cyber relations are better than they have ever been. In promises and in action, the two sides are talking, cooperating, and, more importantly, finding areas of agreement. Although none of this necessarily precludes the possibility of a continued adversarial relationship, these efforts do, at least, suggest the potential for an alternative relationship. China might be continuing to steal from the U.S. in massive quantities, or,

---

133 Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," 15.

134 "China, U.S. discuss int'l norms of state behavior in cyberspace," Xinhua, May 12, 2016, http://news.xinhuanet.com/english/2016-05/12/c_135354264.htm.

135 Mel Gechlik, "Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for U.S. Businesses," Hoover Institution, *Aegis Series Paper,* no. 1706, http://www.hoover.org/sites/default/files/research/docs/gechlik_webreadypdf.pdf.

136 Josh Chin, "Inside the Slow Workings of the U.S.-China Cybersecurity Agreement," The Wall Street Journal (blog), June 15, 2016, https://blogs.wsj.com/chinarealtime/2016/06/15/inside-the-slow-workings-of-the-u-s-china-cybersecurity-agreement/.

as Adam Segal points out, the "absence of evidence is not evidence of absence;[137] that part may or may not have changed. But overall, efforts and actions on the part of the CCP suggest an effort that extends past the stipulations. In other terms, the impact of the Agreement is broad, not narrow.

[137] Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later," Council on Foreign Relations (blog), September 28, 2016, https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

III. VOLUME OF ATTACKS

A. INTRODUCTION

In Chapter I, this thesis briefly discussed the literature surrounding the changes in cyber trends following the 2015 U.S. China Cyber Agreement (Agreement). Analysts generally fell into one of three categories on how to see the results of the Agreement: optimistic, pessimistic, or uncertain. While offering their respective opinions, however, nearly every source cited the same FireEye report as their evidence and did not perform any deeper analysis into the data. Particularly given the reliance on FireEye's data, one should expect derivative users would provide a more thorough analysis, however, none of the sources test or critically analyze FireEye's data. How quickly are changes occurring? Are the changes stable from month-to-month? As a consequence, there could be significant holes in their findings and conclusions. Chapter III, thus, revisits the data to fill the gaps in analytical knowledge by using a wider range of sources and data would not significantly reduce the level of cyber espionage instances or damages. Additionally, Chapter III performs a more rigorous examination of the data, investigating the different rate of change from pre- and post-Agreement periods. Section II re-examines FireEye's data and provides a more thorough investigation of their findings. Section III then analyzes data from Hackmageddon, a third-party source, to test against FireEye's data. Last, Section IV discusses parallel trends through an examination of other, more qualitative, sources and data.

In the end, this chapter finds that the results of the Agreement did not cause a decline in volume of attacks; however, it did play a significant role in accelerating and stabilizing change. The trend of a declining volume of cyberattacks began much earlier than the Agreement, suggesting other events, such as President Obama's threat of sanctions, more accurately represent the cause for the change in Chinese behavior. As a result, the Agreement was likely not a watershed moment. The volume of attacks, however, declined at a greater rate and with less volatility in the post-Agreement period. Additionally, parallel trends partially refute other counter-arguments that claim increased sophistication of Chinese attacks account for the drop in volume. Consequently, the

lower, more consistent level of cyberattacks give reason to believe the Agreement was successful in changing Chinese behavior and for U.S.-China cyber relations to progress optimistically.

B. FIREEYE

As a starting point, it seems prudent to revisit and examine the data in FireEye's report, "Redline Drawn."[138] FireEye claimed their data showed a "notable decline in China-based groups' overall intrusion activity against entities in the U.S. and 25 other countries" that actually began in 2014, prior to the Agreement.[139] As evidence, the group provided a graph showing a declining trend of attacks in "Active Network Compromises Conducted By 72 Suspected China-Based Groups By Month."[140] After a closer examination of their data, this chapter supports much of their same conclusions. Since the Agreement, there has been a positive and promising trend on Chinese behavior in cyberspace, but also much uncertainty. To echo the words of former Director of National Intelligence James Clapper, the "jury is out."[141]

1. Data

Three graphs follow. Figure 4 is the graph from in FireEye's report. Figure 5 and 6 are graphs recreated from data visually extrapolated from FireEye's graph with Figure 5 covering the complete timeline and Figure 6 covering from after the Agreement in September 2015.

---

138 FireEye, "Redline Drawn: China Recalculates its use of Cyber Espionage" (special report, FireEye, June 2016), https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

139 Ibid.

140 FireEye, "Redline Drawn."

141 Michael E. O'Hanlon and James B. Steinberg, "The Trump-Xi summit: A Rocky Relationship Takes Center Stage," Brookings, April 07, 2017, accessed May 15, 2017, https://www.brookings.edu/blog/order-from-chaos/2017/04/07/the-trump-xi-summit-a-rocky-relationship-takes-center-stage/.

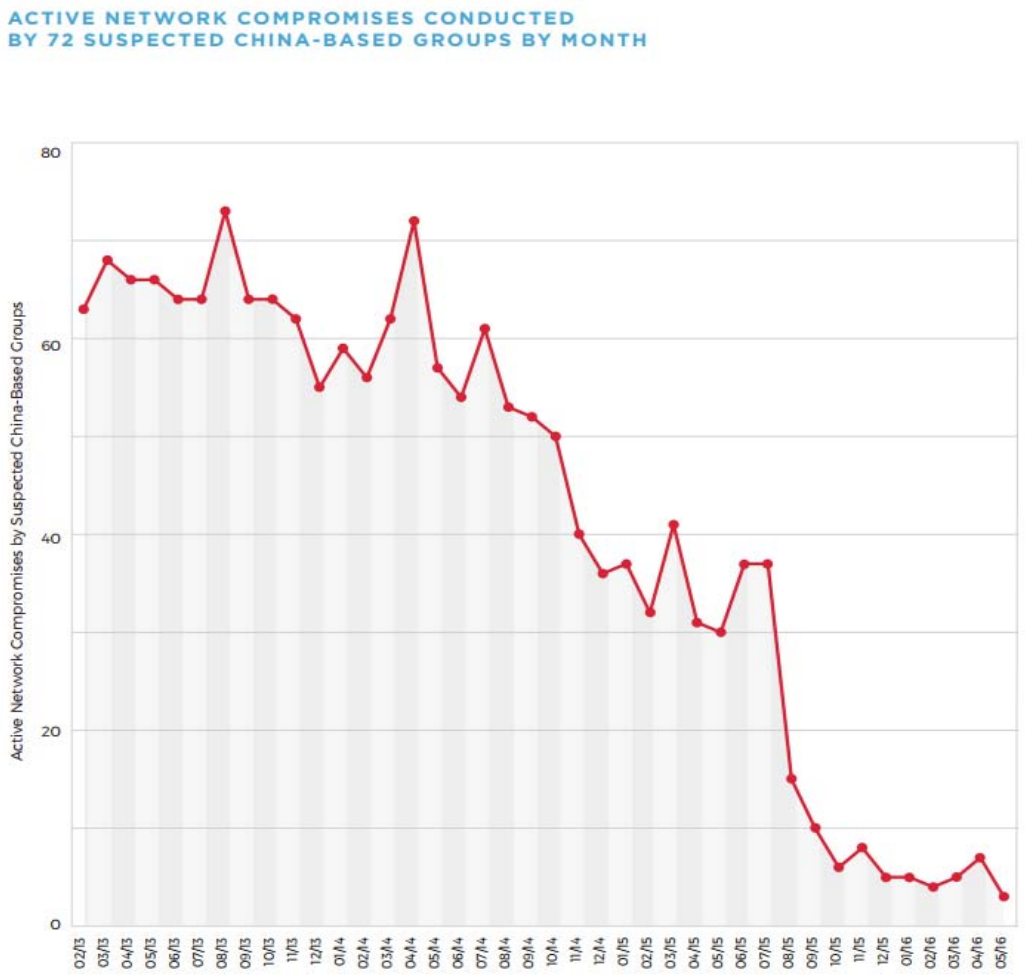


Figure 4. Active Network Compromises.[142]

FireEye's graph covers from February 2013 to May 2016. From Figure 4, one can see a trend in the decline of cyberattacks starting as early as two years prior to the Agreement. This trend, as FireEye and other analysts argue, is evidence that the Agreement is not a major achievement. The volume of attacks was already dropping, therefore making the Agreement costs China very little. Another view, however, is that the Agreement deepened Chinese commitments toward ceasing attacks. As backed by a major drop in attacks from July 2015 to September 2015, the data suggests that the Agreement, while not a cause for decline, made a significant impact itself by accelerating

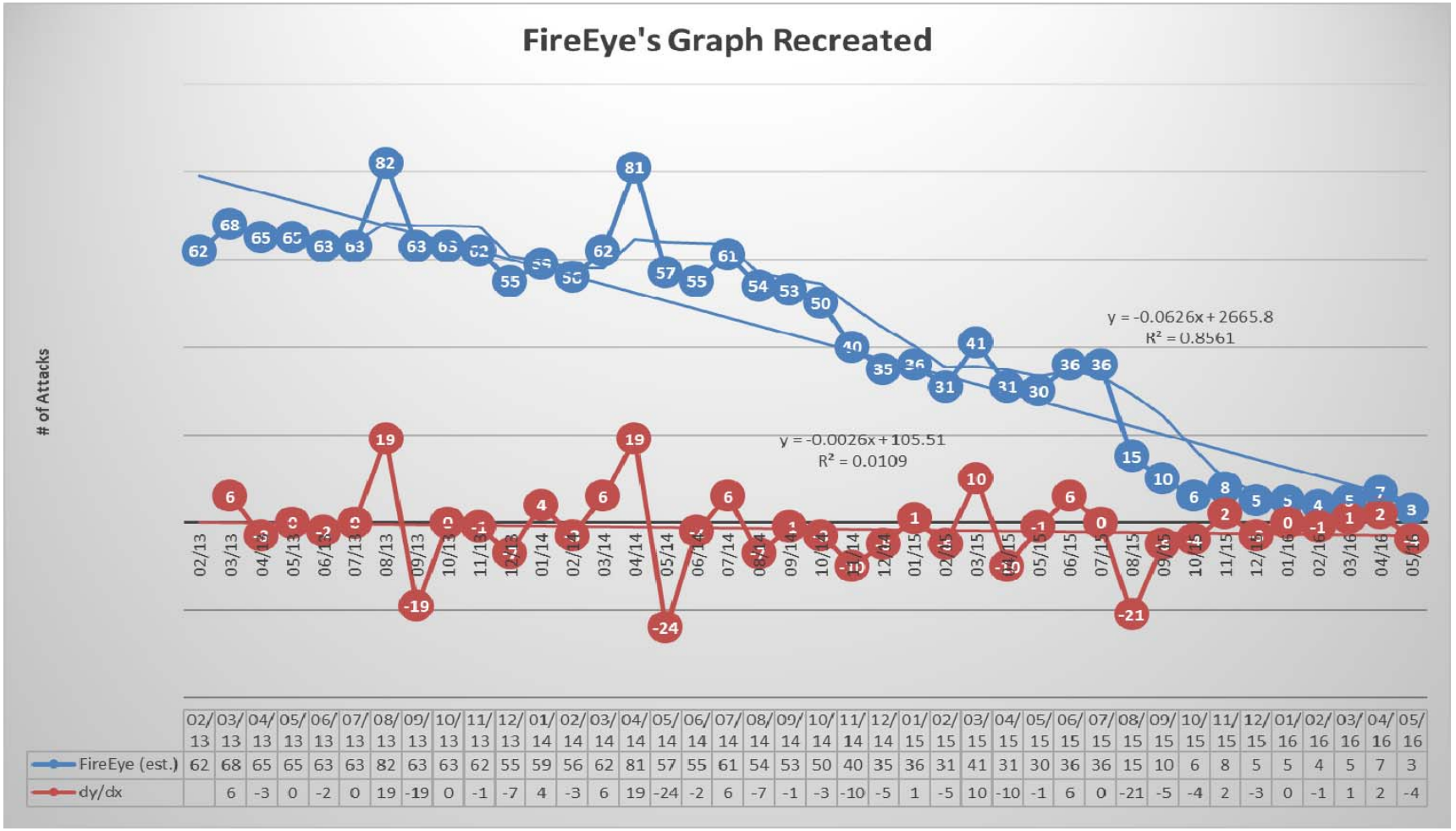
142 FireEye, "Redline Drawn."

change. These observations, however, are fairly speculative; the data can be examined more closely for more solid evidence.

Figures 5 and 6 can be read as follows. The line in blue shows estimated numbers of the volume of attacks from FireEye's report per month. The line in red displays the change in attacks from month to month; positive values indicate an increase in number of attacks whereas negative values indicate a drop. Furthermore, linear equations derived from each set of data display the overall trend for both the blue and red lines. Lastly, the equations provided display the linear equation and R-squared value for each line.[143]

At a glance, no strong correlation or pattern appears from month to month. Visually, there are no consistent cyclical patterns of attacks increasing or falling. Increases in attacks and falls are neither linear nor consistently pace against a previous month. For instance, the only consistent stretch of drops was from August 2014 to December 2014; otherwise, drops and rises occurred intermittently. Additionally, each year from 2013–2015 had 4, 5, and 4 months of increased attacks, respectively. While these statistics show very little, however, a closer analysis of the data reveals far more.

[143] A caveat, however, regarding the *b*-value, or intercept value: the size of the intercept is displayed for the both linear equations, but neither play a role in this analysis. Rather, the focus is on the *m*-value, or slope coefficient, and R-squared value.



	02/13	03/13	04/13	05/13	06/13	07/13	08/13	09/13	10/13	11/13	12/13	01/14	02/14	03/14	04/14	05/14	06/14	07/14	08/14	09/14	10/14	11/14	12/14	01/15	02/15	03/15	04/15	05/15	06/15	07/15	08/15	09/15	10/15	11/15	12/15	01/16	02/16	03/16	04/16	05/16
FireEye (est.)	62	68	65	65	63	63	82	63	63	62	55	59	56	62	81	57	55	61	54	53	50	40	35	36	31	41	31	30	36	36	15	10	6	8	5	5	4	5	7	3
dy/dx		6	-3	0	-2	0	19	-19	0	-1	-7	4	-3	6	19	-24	-2	6	-7	-1	-3	-10	-5	1	-5	10	-10	-1	6	0	-21	-5	-4	2	-3	0	-1	1	2	-4

Figure 5. FireEye's Graph Recreated.[144]

144 Adapted from: FireEye, "Redline Drawn."

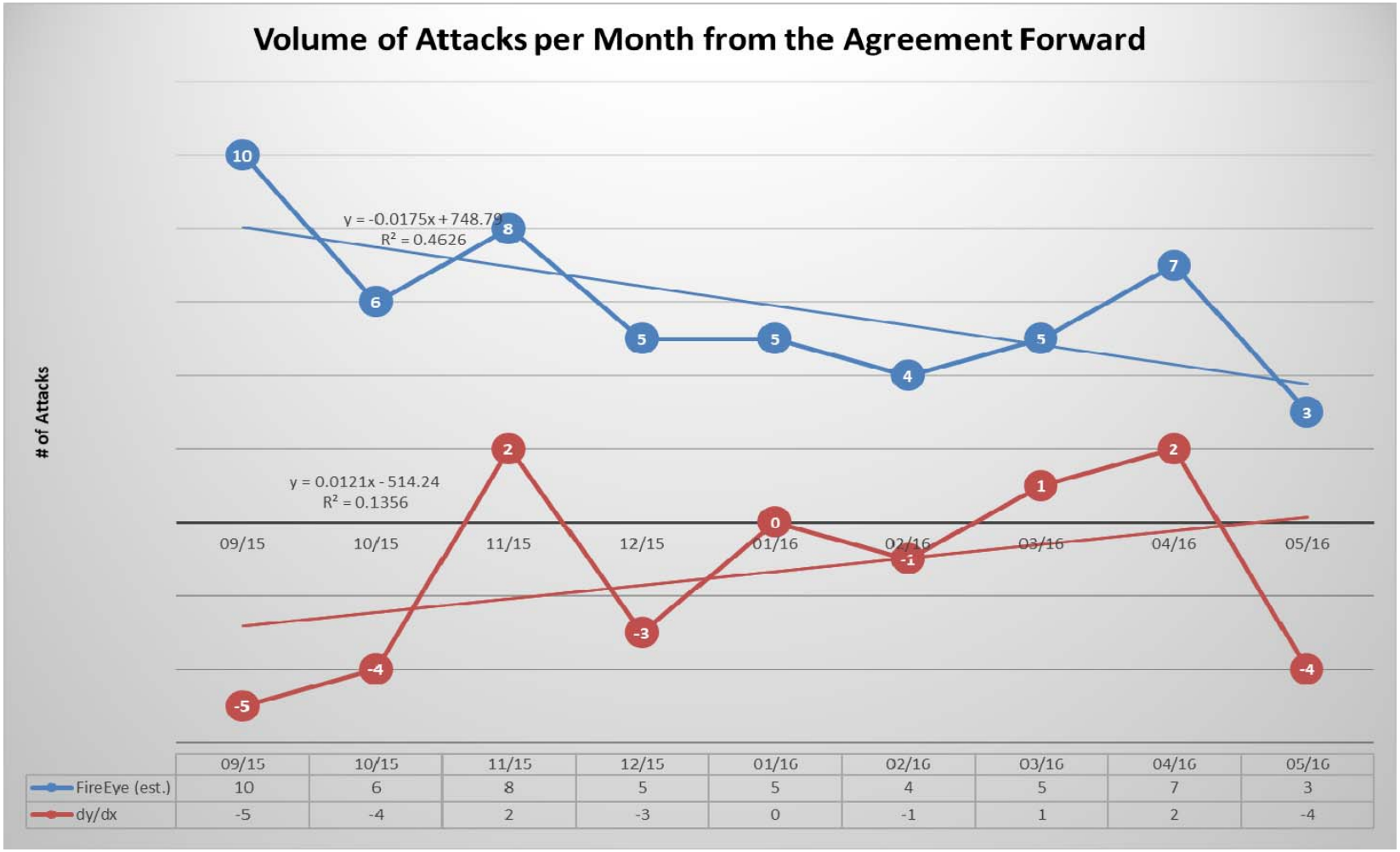


Figure 6. Data from the Agreement Forward.[145]

145 Adapted from FireEye, "Redline Drawn."

2. Evidence of the Agreement Causing Change Beneficial to the United States

The data, for the most part, paints a promising picture of the Agreement. First, looking at Figure 5, the decline in overall attacks is significant. The slope formula for the trend line is:

$$y = -0.0626x + 2665.8$$

With an *m*-value of -0.0626, the monthly drop in attacks occurs at a rate around 2.4, a rate fast enough to not be dismissed. For example, if the value had been closer to zero like -0.000626, the same result would take 100 times longer. Additionally, the trend line also shows a R-squared value of 0.8561. While a high value does not necessarily mean the derived linear function fits the data perfectly, it does suggest a moderate degree of confidence that the trend line, overall, accurately represents the data.

Secondly, the derivative function of Figure 6 also shows there is a relatively and increasingly consistent trend in the decline of attacks. The slope formula for this function is:

$$y = 0.0121x - 514.24$$

Unlike the previous *m*-value, this figure is closer to zero, which in this case is promising for the United States. Since the value is small, the rate of change, or variance from month to month, is consistent. If the value was large, than making a predictive analysis becomes increasingly difficult as the rate of change would be inconsistent. Instead, that value is small, which coupled with an overall negative *m*-value represents a consistent drop in the number of attacks.

Third, while the data in Figure 7 validates FireEye's earlier claim that the Agreement is simply part of sweeping changes in Chinese behavior, the data also suggests the Agreement played a significant part in itself.

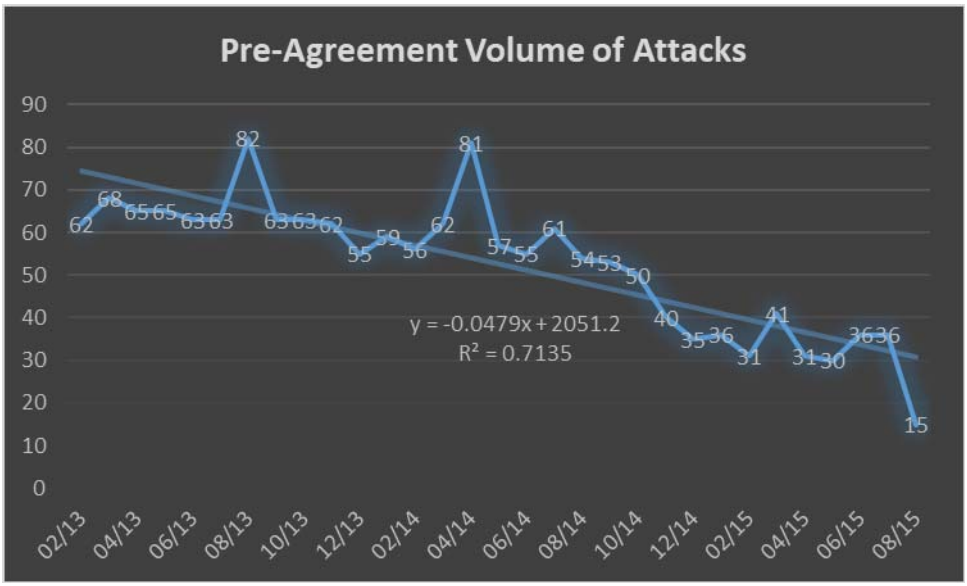


Figure 7. Pre-agreement Volume of Attacks.[146]

Up until the Agreement, the rate of decline was -0.0479. Comparatively, the rate following the Agreement was -0.0175, thus continuing a declining trend of the volume of attacks. While a smaller rate of change, -0.0175 vs -0.0479, the relative drop is much larger. Taking a nine-month difference from December 2014 to August 2015, there was a drop from 35 to 15 attacks and from September 2015 to May 2016, there was a drop from 10 to 3 attacks. In absolute numbers, the drop was much larger prior to the Agreement. However, in terms of ratio, 35:15 is a 2.3:1 ratio, whereas 10:3 is a 3.3:1 ratio, which, in sum, means the drop in attacks is falling faster than prior to the Agreement. Or, in terms of percentage, drops of 57% and 70% respectively. Therefore, it seems that though China likely made the Agreement with a decline of attacks already taking place, this data suggests that the Agreement also provided positive U.S. feedback to bolster a change in Chinese behavior.

Lastly, data shows there is an increasing level of consistency that occurs most notably in September 2015, the same month as the Agreement. Table 1, Column 2 provides a five-month rolling standard deviation in attacks. Column 3 then provides a five-period rolling average of the standard deviation.

146 Adapted from FireEye, "Redline Drawn."

Table 1. Five-Month Rolling Standard Deviation.[147]

	Std. Dev.	Avg
02/13	24.07615	
03/13	2.160247	9.724692
04/13	7.25718	6.479176
05/13	7.494442	7.856731
06/13	7.635444	8.272913
07/13	7.848567	7.48583
08/13	9.04802	6.636974
09/13	9.338094	6.971992
10/13	3.559026	7.120618
11/13	3.391165	7.21123
12/13	9.523655	8.442618
01/14	9.791152	9.763051
02/14	9.791152	9.976496
03/14	9.715966	8.766597
04/14	9.993331	8.202162
05/14	10.59088	8.1832
06/14	3.741657	7.917354
07/14	6.968979	7.558346
08/14	9.621157	8.120993
09/14	8.664102	7.581988
10/14	8.795832	6.496804
11/14	6.554896	5.616431
12/14	4.273952	4.709712
01/15	4.195235	5.199843
02/15	4.262237	6.567364
03/15	4.262237	8.418794
04/15	9.005554	10.34267
05/15	11.11156	11.82146
06/15	13.45239	10.79409
07/15	13.88164	9.021963
08/15	11.65619	6.607167
09/15	3.868678	4.131948
10/15	2.250926	2.066543
11/15	1.378405	1.616009
12/15	1.505545	1.40437
01/16	1.32916	1.417353
02/16		1.32916
03/16		
04/16		

[147] Derived from: FireEye, "Redline Drawn."

As shown in Table 1, prior to the Agreement, there was a high amount of variation between the numbers of attacks. With standard deviation values ranging around 3 to 24, it was difficult to predict how much attacks would rise or fall. One month could see a drop of 10 attacks or an increase of 3 or vice versa. Since the months alternate between increases and decreases in numbers, variation paints a picture of inconsistency and unpredictability from month to month. After September 2015, however, variance takes a sharp dive. From the Agreement forward, variance remains sub-4.0 and averages around ~2.0. As a result, cyberattacks per month are more consistent and predictable since the Agreement.

Overall, the data confirms two things. One, there is enough evidence to suggest the drop in attacks is not just a knee-jerk reaction by China, but a consistent outcome. Two, the impact of the Agreement, while not necessarily a cause for the decline, does show promise in stabilizing the low volume of attacks, thereby aiding in confidence to predict the volume of attacks staying low in the future.

3. Uncertainty in the Data and Analysis

While promising, however, the data does still suggest a degree of uncertainty. In Figure 5, the red line's slope coefficient is small, showing a consistent trend, and the R-squared value is also small. This means the correlation between the line and actual data points is also low. In other words, while the slope equation provides an overall trend, it does not accurately represent the data from point to point. For example, if one month was -10 and the following month was +10, the *m*-value would be zero. Overall, there is no change, but, from month to month, there are major swings. Comparatively, if one month was -1 and the following month was +1, the *m*-value is also zero. The *m*-value, while a good measurement of the overall trend, does not provide a metric for variance. Additionally, the same can be said for Functions 3 and 4. All three functions have an R-squared value >.500, indicating a high degree of variance. In sum, while the trend is downward sloping, the large swings in attacks from month to month also mean the trend could quickly reverse.

Furthermore, Function 4 displays a positive trend line and a positive *m*-value of 0.0121. This means there is a slowdown in the drop of attacks with the possibility of a

reverse trend, a rise in attacks. Therefore, given the timeline's parameters are only from the Agreement on, the data suggests the Agreement may not have the continuous effect of lowering the volume of attacks from its current level.

Despite the variation and room for uncertainty, however, the strength of the data still favors a positive and promising impact. Even with R-squared values under 0.500 and a possible slowdown in the drop in the volume of attacks, the deep dive into FireEye's data still shows a promising trend rather than an increase in volume or return to previous levels.

C. HACKMAGEDDON

Given such promise, one would also expect an impact on global trends as China is often referenced as the largest perpetrators of cyberattacks. This presumption, however, is not a well-established fact. In 2012, Akamai's quarterly "State of the Internet" report sparked public fear as China accounted for more and more of the "world's computer-attack traffic," ending the year with 41% of the global total.[148] Other critics, including the Chinese Defense Ministry, dispute these claims and instead argue the United States is the top actor.[149] Neither side, however, offers compelling or definitive evidence to prove their point.

While exact numbers or even solid estimates on which nations or countries are the largest perpetrator of cybercrimes do not exist, there are some consistent themes. The United States, China, and Russia generally head the list of source countries as seen in

[148] Mark Milian and Jordan Robertson, "China-Based Cyber Attacks Rise at Meteoric Pace," Bloomberg, April 23, 2013, accessed August 21, 2017, https://www.bloomberg.com/news/2013-04-23/china-based-cyber-attacks-rise-at-meteoric-pace.html.

[149] "The Us Government Might Be The Biggest Hacker In The World," Reuters, last edited May 12, 2013, accessed August 21, 2017, https://www.rt.com/usa/us-hacking-exploits-millions-104/; "Hackers R U: China Ranks Us As Top Source Of Cyber Attacks This Year," last edited March 10, 2013, accessed August 21, 2017, https://www.rt.com/news/china-blames-us-hacking-051/.

reports by Symantec, Norse, McAfee, TrendMicro, and Akamai.[150] Almost every report identified each of the three countries are as a major actor, whether the attack was DDOS, botnet, or other form. Thus, the forthcoming analysis assumes China plays a significant part in terms of global attack numbers. In that case, if China-based cyberattacks are indeed on a major decline, then cyberattacks on a global trend should also show an impact, even if it does not also show a decline.

On the other hand, this analysis assumes that the level of attacks is relatively consistent. Expecting a change in the level of global cyberattacks if China's behavior has changed makes the assumption that other actors' behavior remains within expectations. It is possible, however, that other countries underwent significant changes themselves, potentially offsetting any changes by China. If Chinese attacks dropped by 20, an aggregate increase from other countries could have offset China's decrease globally. Conversely, if Chinese attacks increased by 20, an aggregate decrease would explain the limited net change.

Thus, it is possible that a void left by a decline in attacks by China could be filled by other actors. For example, in the case of fishing in the United States, setting limits on catching fish often resulted in overall increases.[151] Fisherman who normally caught below the limit were seemingly incentivized to catch their daily limits. Thus, by using a similar logic, other actors could, plausibly, increase cyber activities in ways that counter-balance China's restraint. For the most part, however, what the data shows is paralleling behavior in the opposite direction: as the volume of cyberattacks by Chinese actors rose, the volume of cyberattacks by other actors also rose. This general correlation does not necessarily mean some states are following other states' lead, but simply that the trend

---

150 "Global Perspective," Norse, December 12, 2015, accessed August 21, 2017, http://www.norsecorp.com/wp-content/uploads/2015/12/December-2015-global-stats.pdf; "The Geographical Distribution Of Cybercrime," Europol, accessed August 21, 2017, https://www.europol.europa.eu/iocta/2015/distribution.html; Red24, "Cybercrime Top 10 Countries Where Attacks Originate," British Bankers' Association, accessed August 21, 2017, https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+countries+where+attacks+originate+-++2015.pdf; Akamai, "State of the Internet/Security: Q2 2017 Report," *Akamai* 4, no. 2 (2017), https://www.akamai.com/us/en/multimedia/documents/state-of-the-Internet/q2-2017-state-of-the-Internet-security-report.pdf.

151 Donald Leal, "Saving Fisheries with Free Markets," *The Milken Institute,* February 2006, http://www.relooney.com/NS3040/0_New_824.pdf.

for individual countries generally parallels global trends as well. Furthermore, although the evidence is far from suggesting that other states may follow more restrained Chinese behavior, at the very least other states are unlikely to react to a drop in Chinese attacks by increasing their own attacks solely for that reason.

Data from Hackmageddon, however, throws an interesting wrench into that parallel line of thinking. Section III explains overall cyberattack data shows little change and little consistency since 2014, thus making the results even harder to interpret.

1. Data

Since 2011, Paolo Passeri, founder of Hackmageddon and a Consulting Systems Engineer Security for OpenDNS, has kept a running log of cyberattacks. Although unverified, his blog offers the only open-source archive of cyber-attack data, and so offers a measurable source of intelligence. And although the data is global, it can be utilized to extrapolate a level of confidence as to whether cyberattacks from China have fallen enough to impact global numbers.[152]

The following graphs, similar to the methods used with FireEye's data, show monthly attack data along with the associated derivative function and regression lines. Figure 8 is the data broken down from Passeri. The combination of Passeri's data into a single data set is displayed in Figure 9. Passeri's data is further broken down by year in Figures 10, 11, 12. Last, Passeri's data is split into two periods, pre- and post-Agreement, in Figures 13 and 14.

[152] The following analysis assumes cyberattacks from the rest of the world are constant. This assumption, if unlikely, is neutral: deviations in either direction would have opposite implications for the analysis. For example, if cyberattacks from the rest of the word increased in this time period, then the following analysis will actually underestimate the impact of decline in attacks from China.

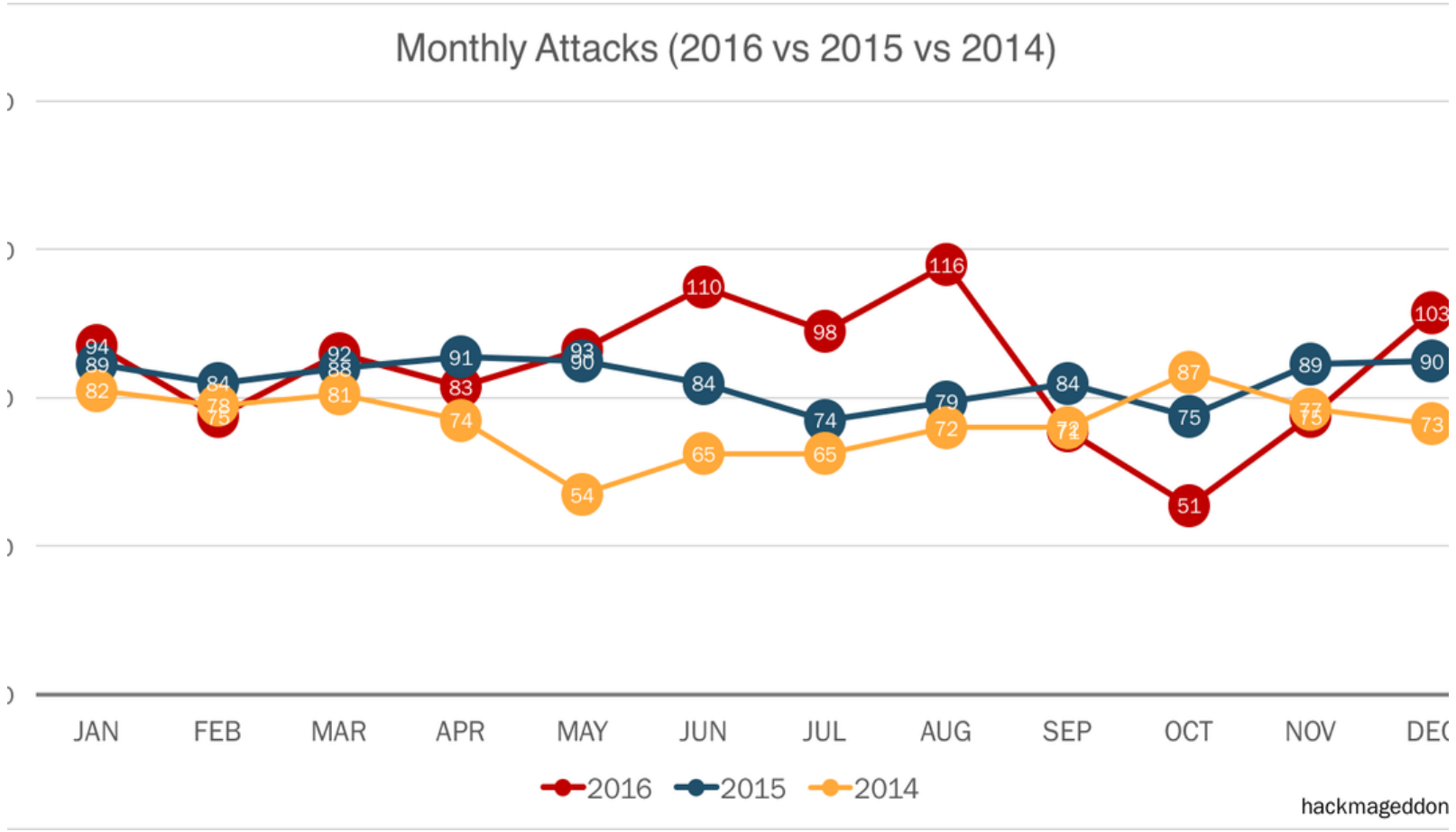


Figure 8. Number of Attacks from 2014–2016.[153]

[153] Paolo Passeri, "2016 Cyber Attack Statistics," January 19, 2017, accessed April 28, 2016, http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/

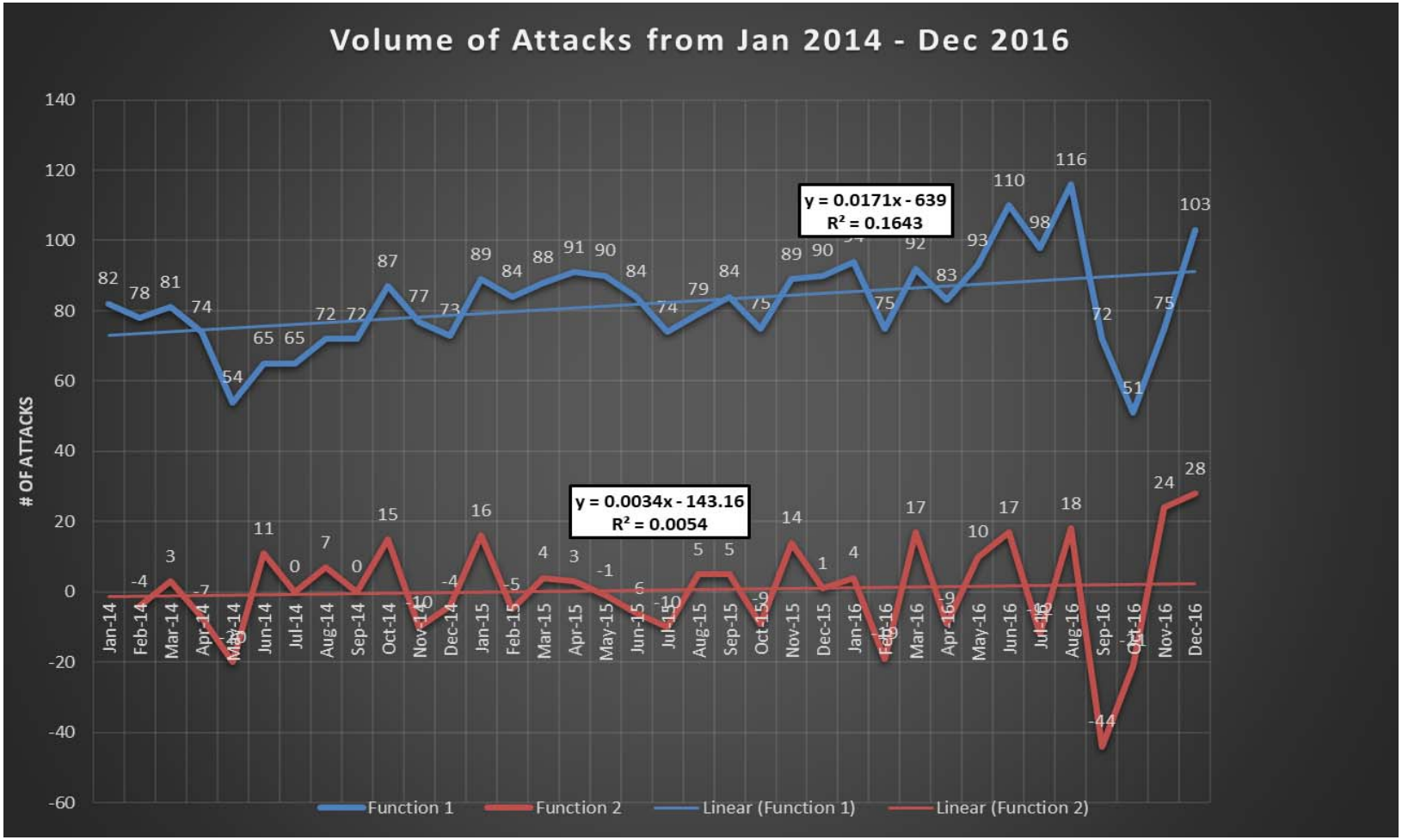


Figure 9. Volume of Attacks from Jan 2014 - Dec 2016.[154]

154 Adapted from: Passeri, "2016 Cyber Attack Statistics."

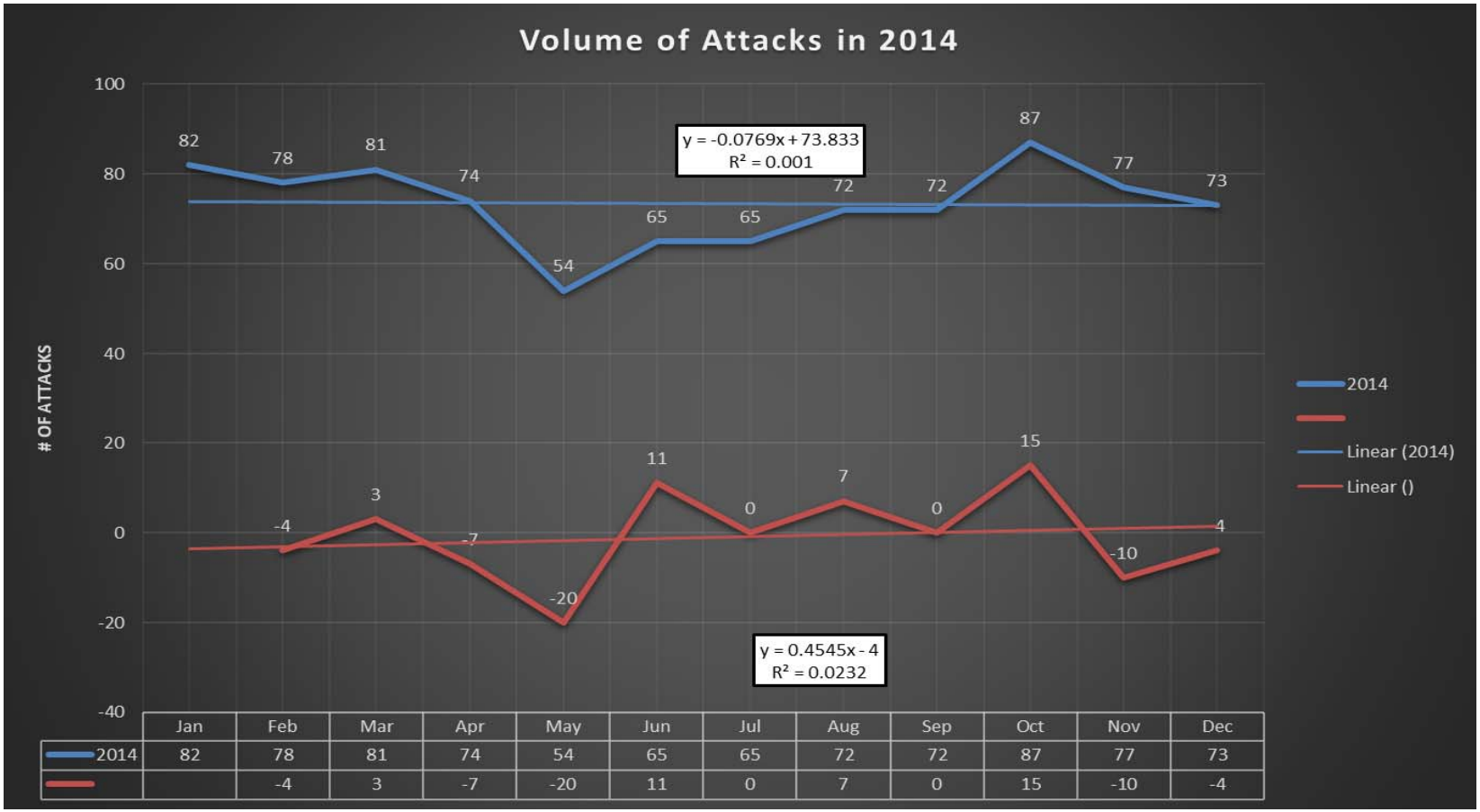


Figure 10. Volume of Attacks in 2014[155]

[155] Adapted from Passeri, "2016 Cyber Attack Statistics."

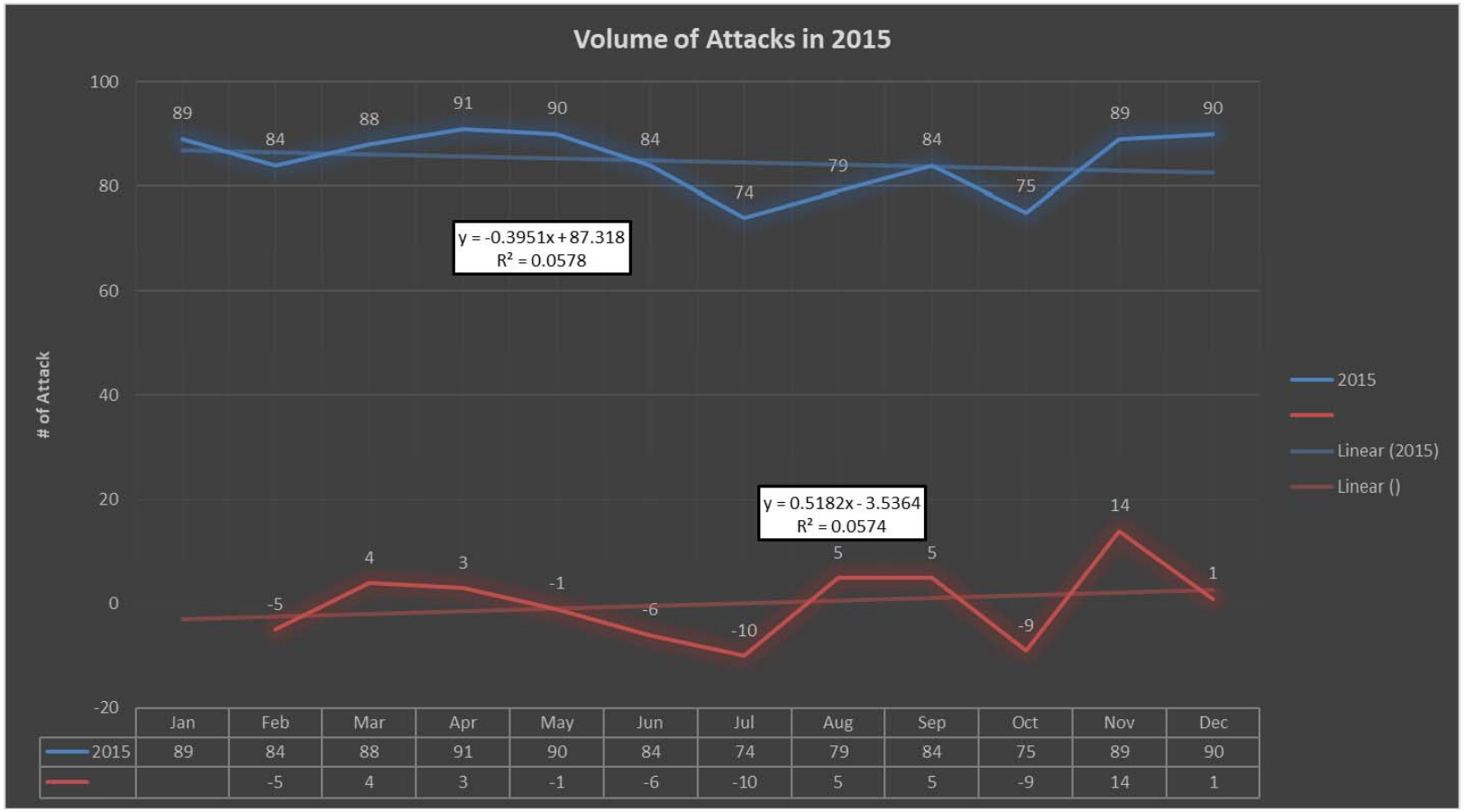


Figure 11. Volume of Attacks in 2015[156]

156 Adapted from Passeri, "2016 Cyber Attack Statistics."

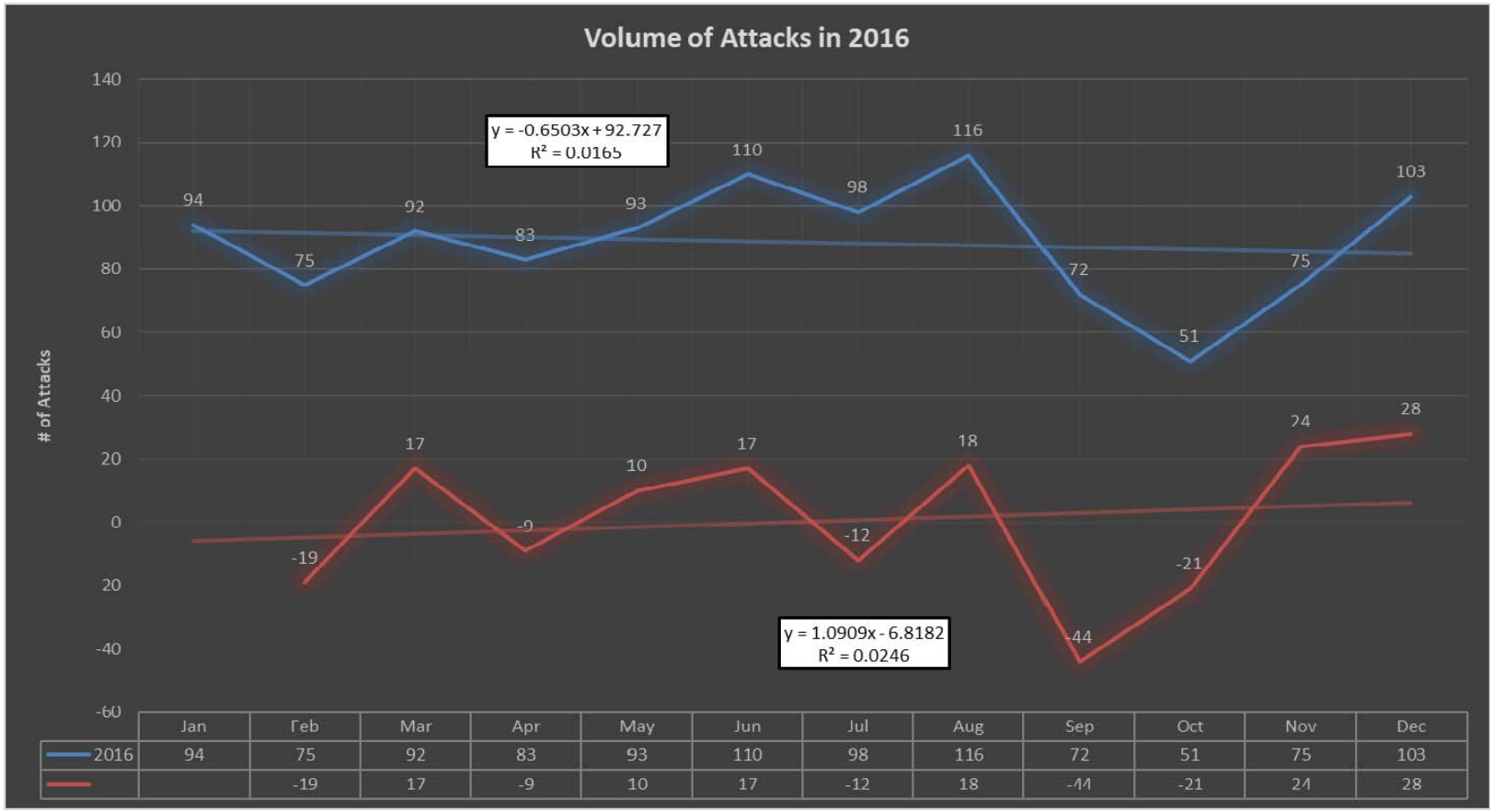


Figure 12. Volume of Attacks in 2016.[157]

157 Adapted from Passeri, "2016 Cyber Attack Statistics."

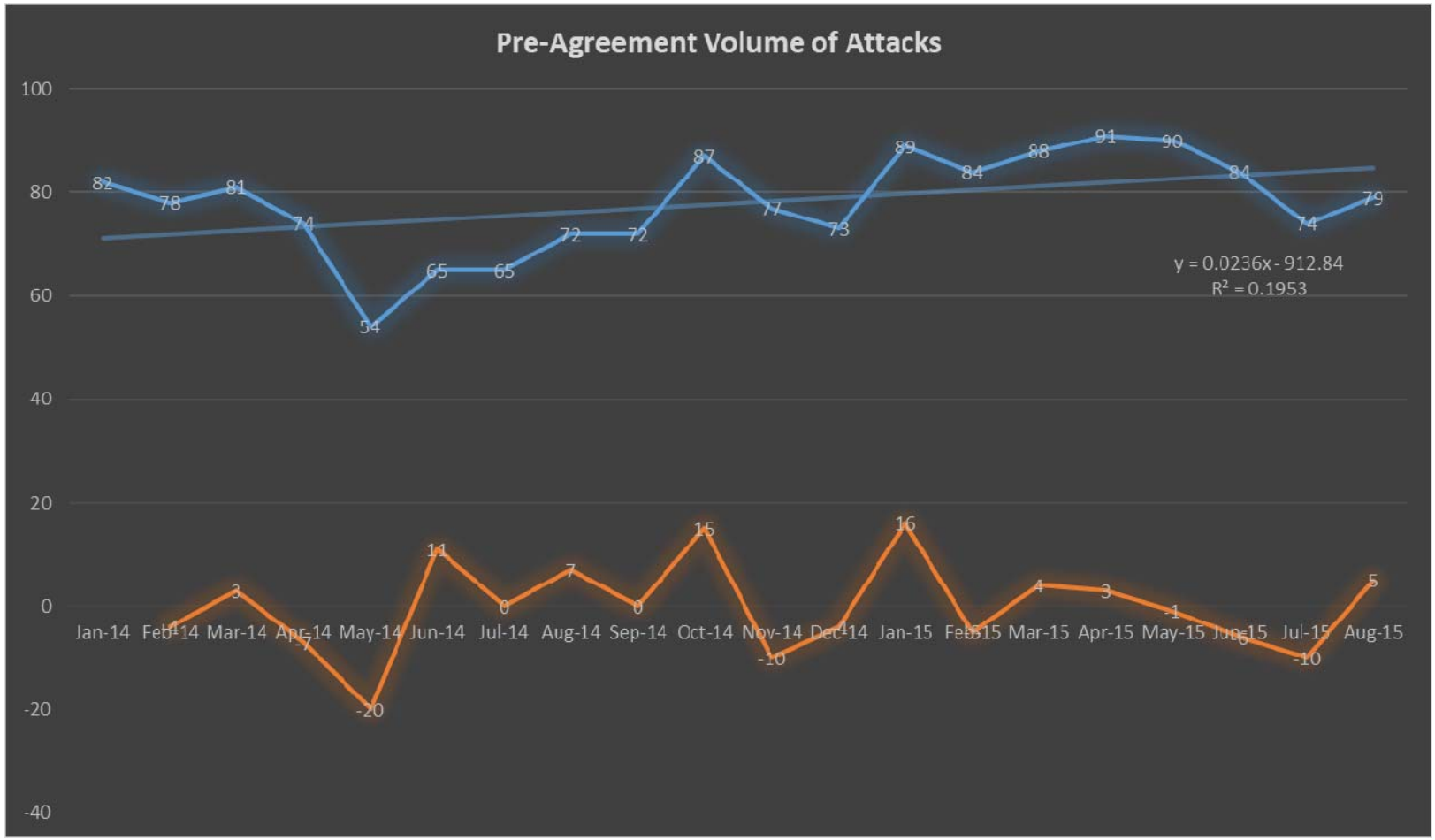


Figure 13. Pre-agreement Volume of Attacks.[158]

158 Adapted from Passeri, "2015 Cyber Attack Statistics."

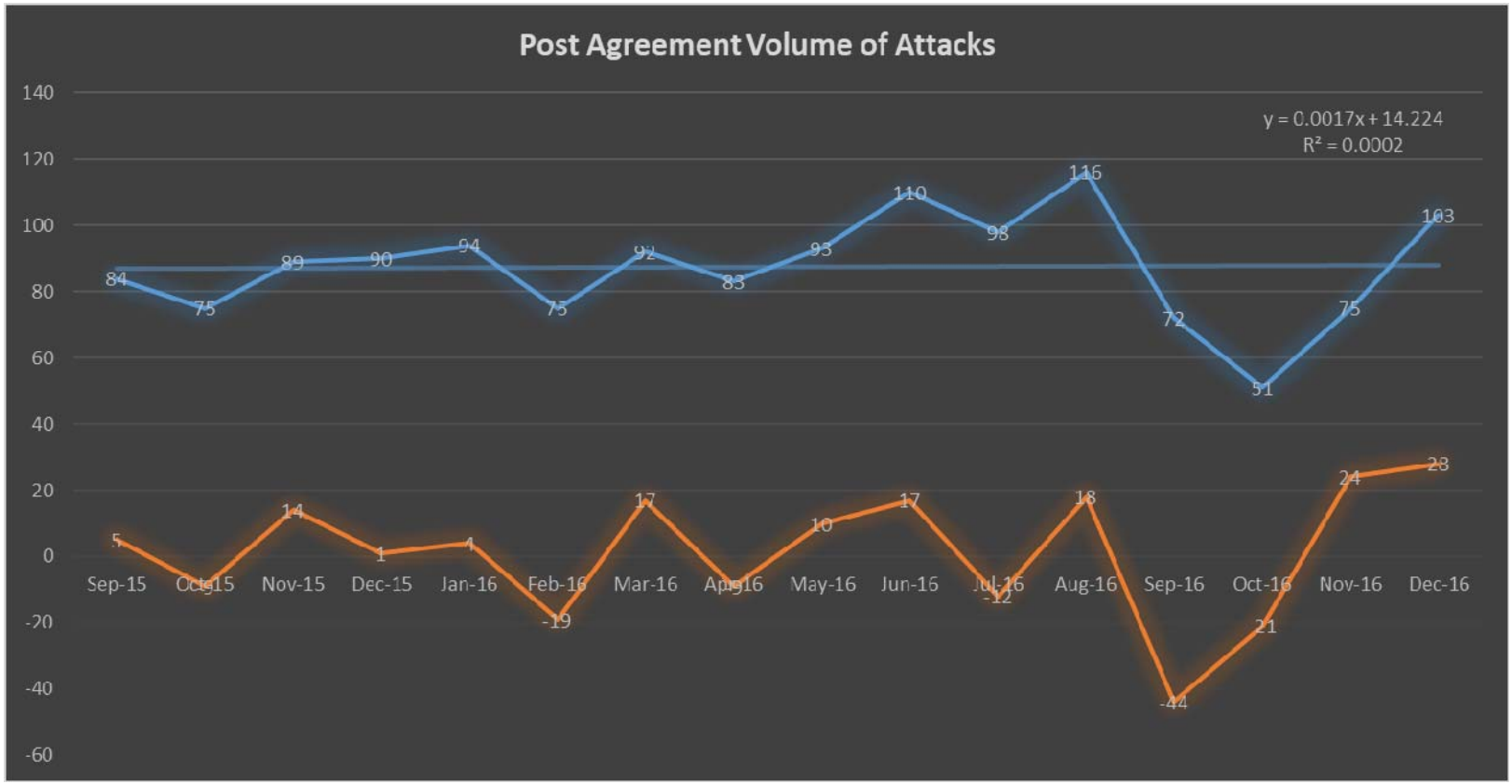


Figure 14. Post-agreement Volume of Attacks.[159]

[159] Adapted from Passeri, "2015 Cyber Attack Statistics."

2. Evidence of the Agreement Causing Change Beneficial to the United States

Similar to FireEye, data from Hackmageddon does provide some promising results. Comparing the pre- and post-Agreement periods, the rate of change in is decreasing. Prior to the Agreement, the volume of attacks increased at a rate of 0.0236 compared to 0.0017 in the period following. In other words, the rate was seven times lower post-Agreement. Thus, the data suggests a potential change in behavior following the Agreement.

Furthermore, in support of the judgment that the Agreement has had an impact, there also appears to be a significant shift from the year to year trend overall. In 2014, the mean level of attack per month was 73.33. In 2015, the mean was 84.75, and in 2016, the mean was 88.5. Thus, the global monthly mean volume of attack from 2014 to 2015 rose by 16%, but only by 4% from 2015 to 2016. However, because the data is derived from global cyberattacks and not broken out by Chinese attacks specifically, the impact is relative to China's proportion of total attacks. Then, assuming that the behavior of the rest of the world is constant, then these data support a conclusion that Chinese behavior has changed following the Agreement.

While this data also supports FireEye's conclusion that the Agreement is less of a watershed moment as the drop in attacks starts before the Agreement, there is still some evidence the Agreement made an impact, given earlier caveats. If, as some critics argue, the drop in attacks occurs only following punitive actions, there is little explanation as to why the rate of drops increases in 2016 given 2016's absence of punitive actions.

3. Uncertainty in the Data and Analysis

Again, similar to FireEye, data from Hackmageddon provides several conundrums. First, on one side, if one accepts several assumptions—that China is one of the largest perpetrators of cyberattacks, that the volume of Chinese cyberattacks declined significantly, and that the volume of attacks from the rest of the world remained constant – then one would also expect global changes to reflect the changes in Chinese behavior in diluted form. Instead, however, global trends seem to be unaffected. Overall, the *m*-value

is relatively small, 0.0171, indicating there has been little change in the volume of attacks from 2014–2017. This could indicate that the behavior of the rest of the world was not constant, or that the Chinese share of the global volume was relatively smaller. Or it could mean that the Hackmageddon data indicate different Chinese behavior than the FireEye data.

More importantly, however, there is a much larger conclusion one can extrapolate from the data: uncertainty. As discussed previously, a low R-squared value is indicative of high variance, therefore low confidence in the trend. In all of the figures, the R-squared value is miniscule. With values all far below .500, the respective trend lines do not accurately represent the data. It appears that, the broader the category, the less accurate the data. Therefore, while FireEye's data has some measure of reliability, measuring volume of attacks on a global scale is not an entirely reliable way of measuring the Agreement's impacts.

D. PARALLEL TRENDS

Although the data on volume of cyberattacks is fairly limited, alternative data sets suggest that there are parallel trends of a change in Chinese behavior. This section discusses the alternative data sets in two parts. First, it examines the periodic reports by cybersecurity firms. Although they do not necessarily provide quantitative metrics, qualitative statements from each report provide a basic understanding of the cyber environment over time. Second, also covered in these reports are observations of the techniques used by suspected Chinese actors from which one can derive potential trends in sophistication.

1. Data

Other than FireEye and Hackmageddon, only few sources provide open source data detailing the volume of cyberattacks and even fewer sources track where attacks originate and/or their destinations. Providing a list of resources, Rita Tehan's CRS report

lists an extensive table of sources that keep track of cyber incidents and breaches.[160] Many of these sources, like Arbor Network's Digital Attack Map, provide "real-time visualization and map of cyberattacks."[161] Honeynet Project's Honeymap, similarily, also provides a real-time map of cyberattacks around the world. Neither, however, retain a historical database of attacks, only data in real time.

Despite their limitations, these sources do provide valuable information. First, while far from definitive proof, the sources generally reaffirm FireEye's conclusion. Symantec's 2017 "Internet Security Threat Report (ISTR)" states, "detections of Chinese espionage malware dropped considerably following a mutual agreement with the U.S. to not target intellectual property."[162] Their report came eighteen months (Sept 2015 – Apr 2017) after the Agreement but makes the same conclusion. While the report does not provide specific numbers, the authors do state confidence in their results, claiming there is "strong evidence that there has been a marked decline in activity by groups probably associated with China since the agreement was signed."[163] Furthermore, in a testimony to the USCC, James A. Lewis from the Center for Strategic and International Studies (CSIS) adds on, "China appears to be living up to its commitments under the Obama-Xi agreement."[164] While the statement lacks specific details, both Symantec and Mr. Lewis assert definite opinions that Chinese cyber-espionage has decreased since the Agreement.

Furthermore, CrowdStrike, a rival competitor to FireEye, reversed their 2015 position and instead, now confirm that there is a decline in volume of attacks. In October 2015, Dmitri Alperovitch, Chief Technology Officer for CrowdStrike, provided a public

---

160 Rita Tehran, Cybersecurity: Data, Statistics, and Glossaries (CRS Report No. R43310) (Washington, DC: Congressional Research Service, 2015), https://fas.org/sgp/crs/misc/R43310.pdf.

161 "Digital Attack Map," Google Ideas and Arbor Network, accessed May 15, 2017, http://www.digitalattackmap.com/.

162 Symantec, "Internet Security Threat Report" (report, Symantec, April 2017), http://s1.q4cdn.com/585930769/files/doc_downloads/lifelock/ISTR22_Main-FINAL-APR24.pdf.

163 Ibid.

164 James A. Lewis, "China's Information Controls, Global Media Influence, and Cyber Warfare Strategy," Center for Strategic and International Studies, May 4, 2017, https://www.uscc.gov/sites/default/files/James%20Lewis%20May%204th%202017%20USCC%20testimony.pdf.

report of the company's observations following the Agreement.[165] While falling short of claiming the Agreement as a failure, he provided evidence of ongoing cyberattacks from a "variety of different Chinese actors," which others have taken as signs of continued behavior.[166] Since then, however, Mr. Alperovitch's views have reversed. In response to President Obama's claim that "we have witnessed Chinese economic cyber espionage reduced but not eliminated," Alperovitch replied, CrowdStrike "confirms that finding."[167] He even goes as far to call the changes in China's behavior as "the biggest success we've had in this arena in 30 years."[168]

In addition, other nay-sayers, like McAfee, while predicting cyber-espionage attacks "would increase in frequency," seem to ignore their own data.[169] McAfee cites the "Verizon Data Breach Investigations Report" as their source of intelligence. McAfee's 2016 report, referencing Verizon's 2015 data, predicts an increase of attacks but are unsure if the numbers will breach 2014's levels of 548.[170] Verizon, however, reported 2015 and 2016 numbers of 247 and 328, respectively.[171] While a modest increase from 2015 to 2016, these numbers fall far short of 2014's level. In other words, the pessimists have insufficient and questionable evidence to back their position.

In sum, most of the sources support FireEye's conclusion and the ones that do not either lack evidence or ignore the numbers they themselves cite. Symantec and Mr. Lewis

---

165 Alperovitch, "The Latest on Chinese-affiliated Intrusions into Commercial Companies."

166 Alperovitch, "The Latest on Chinese-affiliated Intrusions into Commercial Companies."; Ellen Nakashima, "China Still Trying to Hack U.S. Firms Despite Xi's Vow to Refrain, Analysts Say," Washington Post, October 19, 2015, https://www.washingtonpost.com/world/national-security/china-still-trying-to-hack-us-firms-despite-xis-vow-to-refrain-analysts-say/2015/10/18/d9a923fe-75a8-11e5-b9c1-f03c48c96ac2_story.html?utm_term=.4189a87c6d10.

167 Dmitri Alperovitch, Twitter post, December 16, 2016, 12:03 p.m., https://twitter.com/DAlperovitch/status/809851503347453954.

168 Ken Dilanian, "Russia May Be Hacking Us More, But China Is Hacking Us Much Less," NBC News, October 12, 2016, http://www.nbcnews.com/storyline/hacking-in-america/russia-may-be-hacking-us-more-china-hacking-us-much-n664836.

169 McAfee, "2016 Threats Predictions" (report, McAfee, 2016), https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf.

170 Ibid.

171 Verizon, "2016 Data Breach Investigations Report" (report, Verizon, 2016); Verizon, "2017 Data Breach Investigations Report" (report, Verizon, 2017).

both affirm China's adherence to the Agreement. CrowdStrike, in a reversal of position, now affirms the same. Plus, given another year of data, skeptics have yet to provide counter-evidence or take a position claiming an increase in attacks, choosing, instead, to simply refute positive positions without taking any a stance of their own. The data, however, provides far more evidence to be cautiously optimistic, rather than pessimistic.

2. Sophistication

Several analysts in 2015, including FireEye and McAfee, claimed attacks from Chinese actors would trend toward becoming stealthier and more sophisticated.[172] In the year since their claims, however, the data suggests the opposite. Observed attacks have yet to show signs of increased capability in techniques or methodology. Furthermore, defensive capabilities like digital forensics and the number of sensors have improved, bolstering detection capabilities as well.

FireEye has tracked the China-based group, APT3 (also known as Gothic Panda, UPS Team, and TG-0110), since 2014.[173] APT3, according to FireEye, "is one of the more sophisticated threat groups" and is identifiable given the following characteristics.[174] The group targets the following industries: Aerospace and Defense, Construction and Engineering, High Tech Telecommunications, and Transportation.[175] Their techniques include using zero-day exploits, phishing emails, and exploits in Adobe Flash. More specifically, the group is known to use the payload "Backdoor.APT.CookieCutter (aka Pirpi)."[176] If China, as some argue, successfully centralized their cyber force and now use more sophisticated techniques, one would expect to see a change in methodology.

---

[172] McAfee, "2016 Threats Predictions"; FireEye, "Redline Drawn."

[173] "Advanced Persistent Threat Groups," FireEye, accessed, May 15, 2017, https://www.fireeye.com/current-threats/apt-groups.html#apt30.

[174] Eric Eng and Dan Caselden, "Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign," FireEye, June 23, 2015, https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html.

[175] Ibid.

[176] Ned Moran, Mike Scott, Mike Oppenheim, and Joshua Homan, "Operation Double Tap," FireEye, November 21, 2014, https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html.

In a 2016 update by Symantec, however, APT3 changed very little. The report, "Buckeye Cyberespionage Group Shifts Gaze from U.S. to Hong Kong," APT3 continues to use the same techniques.[177] The group has not used new zero-day exploits, instead relies on "vulnerabilities in Internet Explorer and Flash."[178] Use of zero-day exploits, along with other techniques which will be discussed later, is a key indicator of the level of sophistication a cyber actor possesses. Since APT3 shows little progress in this arena, recent data suggests the group has not improved. In addition, relying on older vulnerabilities in Internet Explorer and Flash also suggest APT3 has not adapted beyond detection, but rather may be lagging behind. Internet Explorer and Adobe Flash are rarely used today. Most estimates today show only 3–13% of all browser usage as Internet Explorer and less than 10% of all website use Flash.[179] The market share in either software is rapidly declining, severely limiting the effectiveness of APT3 efforts. Moreover, APT3 also continues to use the same remote access tool (RAT), Pirpi.[180] APT3 has not progressed into a more sophisticated actor, but rather shows signs of stagnation.

Even taking into consideration APT10, improvements may not be as large as they seem. APT10, or MenuPass Group, is another Chinese cyber espionage group identified by FireEye.[181] Unlike APT3, however, the group shows signs of improvement by adopting new tools, notably HAYMAKER, BUGJUICE, SNUGRIDE, and

---

177 Symantec, "Buckeye Cyberespionage Group Shifts Gaze from U.S. to Hong Kong," September 6, 2016, https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong.

178 Ibid.

179 "Usage of Flash for websites," W3Techs, accessed November 09, 2017, https://w3techs.com/technologies/details/cp-flash/all/all; "Browser market share," NetMarketShare , accessed November 09, 2017, https://www.netmarketshare.com/browser-market-share.aspx?qprid=2&qpcustomd=0; "Web Browser Market Share," W3Counter: Global Web Stats, accessed November 09, 2017, https://www.w3counter.com/globalstats.php; Felix Richter, "Infographic: The Web Is Turning Its Back on Flash," Statista Infographics, December 12, 2016, accessed November 09, 2017, https://www.statista.com/chart/3796/websites-using-flash/.

180 Symantec, "Buckeye Cyberespionage Group Shifts Gaze from U.S. to Hong Kong," September 6, 2016, https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong.

181 "APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat," FireEye, April 6, 2017, https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html.

QUASARRAT.[182] While the signs point toward improvement, the use of QUASARRAT suggests that APT10 has not progressed beyond depending on other coders. Upper tier groups with sophisticated techniques generally do not rely on using scripts made by outside entities. Less capable actors, like script kiddies, on the other hand, do rely on open-source scripts as a springboard to enable their activities. As mentioned earlier, zero-day exploits are key indicators of a sophisticated actor because they are basically unknown to all except the threat actor, making the exploits very effective. Avoiding the use of open-source scripts acts on the same principle. Since QUASARRAT is known, it is identifiable, thus more easily preventable and/or detectable. As a result, reliance on QUASARRAT suggests APT10 does not have the in-house knowledge of exploiting .NET framework, instead limited to creating custom tools that exploit HTTP.

E. CONCLUSION

After closer inspection of the data provided by FireEye and Hackmageddon, it appears that the Agreement was not a watershed moment. FireEye's data indicates that the volume of Chinese cyberattacks was declining prior to the Agreement, suggesting Chinese behavior was likely altered due to prior events such as President Obama's implication of sanctions and the U.S. Justice Department's indictment of PLA Officers. Hackmageddon's data also showed that there was not a significant change in global cyberattacks following the Agreement. Therefore, one can conclude that the Agreement did not likely reverse Chinese behavior.

Although the Agreement appears to be part of a larger change in Chinese behavior, however, the Agreement did seem to play a part in accelerating change. FireEye's data showed that attacks fell more quickly following the Agreement and remained more consistent from month to month, suggesting the CCP is controlling their cyber force in a direction positive for the United States. This positive trend is also reflected globally as the number of attacks is rising less swiftly.

Furthermore, parallel trends help to address some of the potential counter-arguments. One, although FireEye and Hackmageddon offer the only quantitative data

[182] Ibid.

sets, thus making the analysis subject to a source bias, other sources' qualitative data support similar findings. The volume of cyberattacks is falling, not rising. Two, early analysis of continued Chinese intrusions seems to be mistaken; most notably, CrowdStrike changed positions from stating Chinese cyberattacks were ongoing to confirming observations of a drop in suspected Chinese-based intrusions. Last, current trends do not support claims of China moving toward a Russian model. Instead, Chinese actors seem to utilize similar TTP, thus dispelling some of those fears.

In sum, the Agreement did not cause a reverse in China's behavior, but likely helped accelerate China's commitment toward cooperating with U.S. goals of stemming the problem of China's cyberattacks. A lower, more consistent baseline of cyberattacks from China will be harder to ignore in future talks. If the volume of Chinese cyberattacks returns to previous levels, the U.S. can use post-Agreement levels as leverage for what can be considered normal levels, which, as will be discussed in Chapter V, may have large implications in U.S.-China relations.

IV. SCHMITT ANALYSIS

A. INTRODUCTION

In Chapter III, this thesis reviewed FireEye's data, which is the main data available, and found a positive correlation between a drop in the number of attacks and the Agreement. Further analysis of the data suggests that China's behavior has greater correlation to the Agreement than what some analysts have previously argued. Despite such evidence, however, focusing solely on the number attacks remains a limited way of examining cyberattacks. As some critics argue, a decreased number of attacks does not necessarily mean the damage is any less. A change in China's efforts, for instance, could potentially direct attacks more effectively, thereby increasing efficiency while reducing the volume of attacks. In order to gain a more complete perspective, Chapter IV, therefore, in order to explore those arguments, utilizes and repurposes a different set of criteria, the Schmitt Analysis, a framework designed to assess whether a particular cyberattack justifies the use of force. First, the chapter explains the Schmitt Analysis and its purpose. Section III, then, explains how the Schmitt Analysis can be repurposed, defining the methodology and data sets. Section IV analyzes the data based on the Schmitt Analysis. Last, Section V explains the overall findings.

Ultimately, this chapter finds results similar to Chapter III: the Agreement was not a watershed moment, but an indicator of progress. Although the volume of attacks is important, other factors, including severity of the damage inflicted, also hold significant weight. This chapter's adaptation of the Schmitt Analysis shows that the *severity* of attacks is also falling. Furthermore, rather than a rise in sophistication, the United States is now better able to attribute Chinese actors to a cybercrime. While the results also show these trends emerging prior to the Agreement, the continuing results suggest real change in Chinese behavior.

B. SCHMITT ANALYSIS

Michael Schmitt, a scholar on international law, recognized the inadequacy of current methods of evaluating cyberattacks for applying international law and proposed a

potential alternative. In particular, his 1999 article exploring the jus ad bellum of cyberattacks highlighted the problematic nature of computer network attacks (CNA).[183] Specifically, he noted that international law lacked an adequate mechanism for which to weigh cyberattacks, particularly because the definition of force was rather ambiguous.[184] As a consequence, Schmitt found the UN Charter definition inadequate, questioning whether the definition of force specifically means armed force or whether coercive efforts also count. He reasoned that a universal definition may be "impossible to resolve,"[185] and, as a result, he proposed an alternative analysis that transcended the debate altogether.

1. Criteria

Schmitt expands the evaluation of cyberattacks by looking at seven factors. He explained that these factors could help states assess "whether particular cyber operations amounted to a use of force."[186] The criteria are as follows: *severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility*.[187] Schmitt's description of each criterion follows:

> (1) Severity: Consequences involving physical harm to individuals or property will alone amount to a use of force. Those generating only minor inconvenience or irritation will never do so. Between the extremes, the more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force. In this regard, the scale, scope and duration of the consequences will have great bearing on the appraisal of their severity. Severity is self-evidently the most significant factor in the analysis.
>
> (2) Immediacy: The sooner consequences manifest, the less opportunity States have to seek peaceful accommodation of a dispute or to otherwise

183 Michael N. Schmitt, "Computer Network Attack And The Use Of Force In International Law: Thoughts On A Normative Framework," *Columbia Journal of Transnational Law* 37 (1999): 887–937.

184 Schmitt, "Computer Network Attack," 13.

185 Ibid., 14.

186 Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: National Academies Press, 2010), 151–177.

187 Ibid., 155–156.

forestall their harmful effects. Therefore, States harbor a greater concern about immediate consequences than those which are delayed or build slowly over time.

(3) Directness: The greater the attenuation between the initial act and the resulting consequences, the less likely States will be to deem the actor responsible for violating the prohibition on the use of force. Whereas the immediacy factor focused on the temporal aspect of the consequences in question, directness examines the chain of causation. For instance, the eventual consequences of economic coercion (economic downturn) are determined by market forces, access to markets, and so forth. The causal connection between the initial acts and their effects tends to be indirect. In armed actions, by contrast, cause and effect are closely related—an explosion, for example, directly harms people or objects.

(4) Invasiveness: The more secure a targeted system, the greater the concern as to its penetration. By way of illustration, economic coercion may involve no intrusion at all (trade with the target state is simply cut off), whereas in combat the forces of one State cross into another in violation of its sovereignty. The former is undeniably not a use of force, whereas the latter always qualifies as such (absent legal justification, such as evacuation of nationals abroad during times of unrest). In the cyber context, this factor must be cautiously applied. In particular, cyber exploitation is a pervasive tool of modern espionage. Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target-State's territory, as in the case of a warship or military aircraft which collects intelligence from within its territorial sea or airspace. Thus, actions such as disabling cyber security mechanisms to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force.

(5) Measurability: The more quantifiable and identifiable a set of consequences, the more a State's interest will be deemed to have been affected. On the one hand, international law does not view economic coercion as a use of force even though it may cause significant suffering. On the other, a military attack which causes only a limited degree of destruction clearly qualifies. It is difficult to identify or quantify the harm caused by the former (e.g., economic opportunity costs), while doing so is straightforward in the latter (x deaths, y buildings destroyed, etc).

(6) Presumptive legitimacy: At the risk of oversimplification, international law is generally prohibitory in nature. In other words, acts which are not forbidden are permitted; absent an express prohibition, an act is presumptively legitimate.25 For instance, it is well accepted that the international law governing the use of force does not prohibit propaganda,

> psychological warfare or espionage. To the extent such activities are conducted through cyber operations, they are presumptively legitimate.
>
> (7) Responsibility: The law of State responsibility (discussed below) governs when a State will be responsible for cyber operations. But it must be understood that responsibility lies along a continuum from operations conducted by a State itself to those in which it is merely involved in some fashion. The closer the nexus between a State and the operations, the more likely other States will be to characterize them as uses of force, for the greater the risk posed to international stability.[188]

These seven criteria form the basis of Schmitt's analytical framework and provide a more comprehensive perspective than volume alone on which to judge cyber-attacks in terms of use of force.

Schmitt's seven different factors help overcome the previous pitfalls of other framework(s). First, the seven factors provide definitive questions rather than ambiguous and subjective interpretations of the principles of necessity and proportionality. *Severity* provides a scale of damages. At one end of the scale exist attacks that caused "physical harm to individuals or property," and, at the other end, "those generating only minor inconvenience or irritation."[189] *Directness* measures whether the effects are primary, secondary, and so on.[190] Moreover, *measurability* provides a metric to quanitify the effects of a cyberattack.[191] Having definitive factors removes some of the burden for decision makers. Rather than having to dig through layers of questions like discussing damages under both necessity and proportionality, the Schmitt Analysis already provides the necessary questions.

Crucially, the specificity of the analysis provides a standard to measure cyberattacks. In general, most comparisons of one attack to another do not utilize a standard framework. Arguments, then, vary from discussing their political effects, methodology, and intent, among other criteria resulting in circular conversations. The Schmitt Analysis, in contrast, can be universally applied to all cyber-attacks. Therefore,

---

188 Michael N. Schmitt, "Cyber Operations in International Law."

189 Michael N. Schmitt, "Cyber Operations in International Law."

190 Ibid., 156.

191 Ibid.

comparisons can be made more equally. It is understandable to review each attack on a case-by-case basis, but, without a standard way of comparison, determinations rely on the individuals reviewing the case.

The Schmitt Analysis has also already been effective when applied to cyber-attacks. Keely applied the analysis to the case in Estonia.[192] Each of the seven factors were applicable and helped structure the attack. Ultimately, Keely found that, under severity, there was no physical harm and thus "no *casus belli.*"[193] Foltz also made an analysis of Stuxnet and was also able to apply each of the factors.[194] Stuxnet and Estonia were different in method, purpose, actors, and time, but both authors produced a similar point. The Schmitt Analysis provides a basis by which to accurately describe and evaluate any cyberattack.

C. METHODOLOGY

The Schmitt Analysis, therefore, can be an effective tool in determining differences between one cyberattack and another. In turn, analyzing these changes may reveal indications of changes in a state's behavior, China in this case, and potentially determine whether the state's behavior has changed significantly or not. This section explains how the Schmitt Analysis can be repurposed, where the data is drawn from, and how the data will be analyzed.

1. A. Repurposing the Schmitt Analysis

The Schmitt Analysis has a relatively specific purpose: to determine "whether particular cyber operations amounted to a use of force."[195] As a result, the criteria is geared toward identifying areas of potential tripwires and redlines, the backdrop of which is based on international law. Furthermore, Schmitt intended the framework to evaluate a cyberattack holistically, judging a cyberattack by analyzing all seven criteria together

192 David M. Keely, "CYBER ATTACK! CRIME OR ACT OF WAR" (Strategy Research Project, U.S. Army War College, 2011), 21.

193 Ibid., 22.

194 Foltz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate," 43.

195 Michael N. Schmitt, "Cyber Operations in International Law," 155.

versus individually, to determine use of force. This thesis repurposes the framework slightly: rather than examining whether one given attack crosses a use-of-force threshold, the forthcoming analysis compares sixteen cyberattacks attributed to China (for which there is robust data) to determine whether Chinese post-Agreement behavior in cyberspace has changed.

A discussion of each of the seven criteria's potential in measuring changes to Chinese behavior and how this thesis applies the criteria follows.

a. *Severity:*

As some critics of the Agreement argue, a drop in the value of attacks does not necessarily equate to less damage or less theft by Chinese actors. Instead, as many argue, the drop can also be explained by a change in tactics. Rather than a large number of unsophisticated attacks, Chinese strategy could have shifted, since the Agreement, toward more sophisticated and damaging tools, techniques, and procedures (TTP). As a consequence, analysis determining whether the Agreement has or has not been successful should, if possible, address these arguments, which this particular criterion, *severity*, does.

Severity, as defined by Schmitt, offers a way to measure attacks based on the amount of damage done. Therefore, by measuring the severity of attacks prior to and following the Agreement, the thesis can determine whether the Agreement potentially altered the amount of damage done by a particular operation. If there is a notable decline in the severity of attacks, the data would potentially suggest the Agreement is successful. If, vice versa, severity has increased, critics of the Agreement may be right in that China is simply shifting strategy.

There are, however, some notable pitfalls with measuring severity as a determinant for China's behavior post-Agreement. The following section, Data Sources, discusses that the criteria can only be applied to a limited number of credible cyberattacks, due in part to limited information. This problem is not limited to *severity*, but extends to all of the criteria. Additionally, *severity* lacks an effective way to assign weight to individual attacks. Not all attacks in an operation aim toward the same goal;

some attacks can be more significant than others. Thus, the data could be potentially skewed. As a result, this methodology evaluates a cyberattack as the aggregation of numerous smaller attacks.

b. *Immediacy:*

Immediacy is not the most directly applicable criterion for the purpose of this thesis, but is still useful. As a measurement of cyberattacks crossing the threshold of an act of war, *immediacy* is more useful in the time sensitive nature of decisions regarding war than in longer term changes. It can, however, still be useful in determining a change in Chinese behavior post-Agreement. Whether attacks are executed quickly or slowly provides insight as to the purpose of the attack. Quick strikes suggest efforts are direct and purposeful in nature, potentially meaning Chinese actors have an intended target. Slower strikes suggest attacks follow a "death by a thousand cuts" methodology, stealing information in an opportunistic manner.[196] There are, of course, potentially other causal reasons for why attacks are more or less timely. For example, slow strikes may also mean attackers are attempting to conceal specific actions or may not believe their actions have yet been compromised. As a result, *immediacy* as a criterion may not provide strong evidence of change. Nevertheless, data may still provide some insight.

c. *Directness:*

Measuring *directness* offers a potential way to determine whether there is a shift in the purpose of cyberattacks. Similar to *immediacy*, the more directly related an attack is to a consequence , the higher level of confidence there is toward determining the purpose of an attack. If, for example, a Chinese cyberattack directly stole an industrial secret, the level of *directness* would be very high. If the level of *directness* following the Agreement falls and damages were more secondary or tertiary in nature, the trend would suggest Chinese behavior has positively changed from a U.S. standpoint. A caveat, however, is that, much like *immediacy*, there is some difficulty in establishing what the

196 William C. Hannas, James Mulvenon, and Anna B. Puglisi, Chinese industrial espionage technology acquisition and military modernization (London: Routledge, Taylor & Francis Group, 2013).

change in behavior exactly means. As a result, this criterion, *directness,* is more useful as a supplemental criterion.

d. *Invasiveness:*

Although the specific boundaries of cyberspace are difficult to define, a notion of sovereign territory still exists. The Internet exists via a series of physical infrastructure consisting of routers, servers, computers, and other physical devices. These devices exist in the "real world," meaning that their physical location resides within the boundaries of a particular nation/state. Therefore, though cyberattacks occur within ambiguous territory and in murky jurisdiction, there is still a measurable amount of invasiveness or intrusion taking place. If an attack siphoned data off a server's hard drive housed within U.S. boundaries, there is a high level of *invasiveness.* Alternatively, if data was siphoned off from a transmission from that U.S. server en route to another server, there is a much lower level of *invasiveness.* More simply put, there is a difference between stealing something from someone's home and from taking it from their mailbox.

e. Measurability:

Using *measurability* as a metric is not as useful toward determining sophistication as it is a means to examine potential evidence for how best to respond with soft power. The theft of the F-35 technology, for instance, is more easily measurable because the exact consequences of the information are fairly well known. The exact damage caused by Chinese cyber phishing campaigns, on the other hand, are much more difficult to measure. While a likely correlation between *measurability* and sophistication exists, the proportion of correlation is unknown. The difference in *measurability* levels, however, does offer a different perspective on the trend of cyberattacks. A shift from high to low levels may suggest Chinese actors are taking potential U.S. actions more seriously. Consequently, when, and if, that shift occurs, changes the way one might perceive behavior since the Agreement. If the change only occurs in line with threats of U.S. sanctions, then the Agreement may have had little impact. If, however, the change only occurs following the Agreement, then institutional mechanisms play a larger role than critics might suggest.

f. *Presumptive legitimacy*

There appears to be a clear difference in perspective and/or opinion with respect to cyber espionage. As RAND pointed out, U.S. officials imply that there is a difference between theft of industrial trade secrets and theft of military secrets.[197] According the Agreement, the former should be banned, hence the point of the Agreement, while the latter is more acceptable. China's view, however, does not appear to see the same difference, possibly equating economic theft as a pillar of national security. The Agreement appears to push China toward recognizing a difference, which this particular criterion can measure. Taking the perspective of the U.S., measuring attacks based on whether they are in line with international law or not may offer insight as to whether China may or may not perceive a difference in industry theft versus military theft.

g. *Responsibility/Attributability*

Lastly, *responsibility* originally refers to the role of the state in conducting a cyber operation. As pointed out by Mandiant's report on APT1, even a mountain of evidence does not equate to definitive proof of a state's involvement.[198] As a result, this thesis suggests a slight alteration or, rather, a different interpretation. If one, instead, measures the level to which a particular cyber operation can be attributed to a state actor, one may attain better insight as to whether China is making increased efforts at concealing their attempts. This does not necessarily rule out better control of reigning in freelance or moonlighting hackers, but, coupled with the volume of attacks, it may support or contradict critics' claims that Chinese attacks are moving toward a Russian model

2. Data Sources

At the time of this thesis, a definitive source that compiles cyberattacks attributed to China does not exist. There are, however, five documents that list a number of cyberattacks, which together make up a fairly comprehensive list. They are as follows:

---

[197] Scott Warren Harold, Martin C. Libicki and Astrid Cevallos, *Getting to Yes with China in Cyberspace,* Santa Monica, CA: RAND Corporation, 2016, http://www.rand.org/pubs/research_reports/RR1335.html.

[198] M. I. Center, "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, Tech. Rep, Tech. Rep., 2013.

"Cyber Incidents Attributed to China," "Significant Cyber Incidents Since 2006,""Cyber Attacks on U.S. Companies in 2014," "Cyber Attacks on U.S. Companies Since November 2014," and "Cyber Attacks on U.S. Companies in 2016."[199]

The first document, "Cyber Incidents Attributed to China," is included for two reasons.[200] First, the organization and the authors of the documents represent one of the foremost subject matter experts on the topic. CSIS is a non-profit policy research think tank that covers a litany of subjects, but, rather notably in regards to cybersecurity, is often involved in many international discussions and exchanges. Additionally, James A. Lewis, now Senior Vice-President of CSIS, has covered Chinese cyber policies for several years and, as a result, is often brought in to testify to Congress on the subject; thus, he can be considered one the foremost authorities on the subject. Second, the depth and clarity of the document are superior to any other list. Lewis breaks document into two sections, actions attributed to a specific individual and/or entity and actions attributed to China in general. He is the only one to both identify and separate attacks attributed to China as well as differentiate the attacks by whether the attacker has been specifically identified or not. The list, however, only covers a period from 1991 to 2013. Furthermore, the list does not include attacks potentially attributed to China, thus the data set is fairly limited.

The next document, however, helps bridge those gaps, by providing more data and more recent cyberattacks. CSIS's "Significant Cyber Incidents Since 2006," adds the weight of the organization to support its veracity.[201] In addition, the list is continuously updated by a number of researchers, thus providing as close to up-to-date information as

---

[199] Laura Saporito and James A. Lewis, "Cyber Incidents Attributed to China," Center for Strategic and International Studies, March 11, 2013, https://www.csis.org/analysis/cyber-incidents-attributed-china; CSIS, "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, accessed August 1, 2017, https://www.csis.org/programs/technology-policy-program/cybersecurity/other-projects-cybersecurity/significant-cyber; Riley Waters, "Cyber Attacks on U.S. Companies in 2014," Oct 27, 2014, http://thf_media.s3.amazonaws.com/2014/pdf/IB4289.pdf; Riley Waters, "Cyber Attacks on U.S. Companies Since November 2014," November 18, 2015, http://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014; Riley Walters, "Cyber Attacks on U.S. Companies in 2016," The Heritage Foundation, December 2, 2016, http://www.heritage.org/defense/report/cyber-attacks-us-companies-2016.

[200] Saporito and Lewis, "Cyber Incidents Attributed to China."

[201] CSIS, "Significant Cyber Incidents Since 2006."

possible. While it does not separate attacks attributed to China specifically, the list does include the national origin of the cyberattack when available, thereby allowing this thesis to differentiate attacks for the purpose of this chapter.

The last three documents are generated by the Heritage Foundation's Riley Walters, another U.S. think tank that specializes in policy issues.[202] Walters, a research associate, started his list in 2014 and continues to provide annual updates. Again, while not separating China as the actor specifically, his list does provide an important distinction of cyberattacks on U.S. companies versus foreign companies. The inclusion of these documents provides a secondary source of information, helping to separate source bias as well as to provide more data points to analyze.

Drawing from these five documents, this author then compiled a list of attacks possessing two particular criteria: cyberattacks that potentially originated from or were attributed to China or Chinese actors and cyberattacks whose target(s) were U.S. companies/organizations. Then, from this list, the cyberattacks were again limited down to the attacks with significant research behind them; specifically, attacks with enough reporting data to determine numerical values for each of the criteria from Schmitt Analysis (as explained in the following section). In total, sixteen attacks met the set criteria.

3. Method of Analysis

Borrowing the idea from the research paper, "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System,"[203] this thesis similarly applies a quantitative scale to each of the criteria under the Schmitt Analysis for each cyber incident. The presumption is that applying a quantitative scale permits "any given operation could be described in

---

[202] Waters, "Cyber Attacks on U.S. Companies in 2014."; Waters, "Cyber Attacks on U.S. Companies Since November 2014."; Walters, "Cyber Attacks on U.S. Companies in 2016."

[203] James B. Michael, Thomas C. Wingfield, and Duminda Wijesekera, "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System," in *Proc. of 27th Annual International Computer Software and Applications Conference*, pp. 622–626, November 3–6, 2003.

qualitative terms as being closer to one end of a spectrum or the other."[204] As a result, each criterion was assigned a value of 1–100 with the following goal. Values closer to 100 represent where Chinese actions violated the terms and/or spirit of the Agreement more grossly, whereas values closer to 1 represent actions closer to cooperation.

For *severity,* the values for each attack were assigned based on the suspected economic damages, either actual or attempted. In addition, values were assigned in two different ways. The first method assigned values based on total damages caused. The second method assigned values based on damages on private companies, excluding government and military information. *LuckyCat*, for example, registered a higher score in total damages considering overall damages as the attack primarily targeted military information, however, registered a much lower score in terms of private industry damage considering only damages to the private sector as the malware was not suspected to have impacted the general public as it targeted a specific audience.

For *immediacy*, valuation consisted of two factors: how quickly damages were caused between initial intrusion and actual theft and for what amount of time the attack persisted.

For *directness,* valuation mainly considered whether the theft was a target of opportunity or not. Some analysts have described Chinese cyberattacks as "death by a thousand cuts." Essentially, Chinese methodology consisted of targets of opportunity, stealing information where possible rather than goal oriented. Thus, values to 1 indicate damages created by opportunity and values closer to 100 indicate targeted theft.

For *invasiveness,* valuation consisted of determining where the attacks took place. Lower values indicate theft occurring on Chinese infrastructure. Middle values indicate theft occurring during transmission between different parties. Lastly, higher values indicate theft from networks and computers within the United States. The purpose of this valuation is to differentiate attacks that may have higher or lower deniability. Chinese traffic on Chinese servers, for example, is less incriminating than Chinese traffic on U.S. servers.

---

[204] Ibid.

For *measurability,* valuation consisted of how well damages for an attack can be measured. Low values indicate attacks with reported intrusion(s) but whose theft is relatively unknown. High value, in contrast, indicate attacks with more well-known damages such as the theft of the F-35 data.

For *presumptive legitimacy,* scores are assigned based on whether the target(s) were government/military or civilian targets, lower scores assigned to the former and higher for the latter.

For *responsibility,* scores were assigned as to how well the attack could be tied toward Chinese actors. Higher scores indicate a greater level of attribution and lower scores represent attacks with greater plausible deniability.

In regards to weighting among these factors, the analysis gives more emphasis toward *severity*. *Severity*, as a scale of damage, is, perhaps, the closest parallel assessment to the volume of attacks as the two are linked in many ways. For instance, one way to view the volume of attacks is to equate volume with damage, however, higher volume does not necessarily mean higher damage. Thus, *severity* is a means to cut out the middleman. Therefore, since much of the analysis on the Agreement utilizes volume of attack as the ruling metric, *severity* is weighed more heavily than the other six criteria.

The other six criteria, however, still play an important role, either strengthening or playing spoiler to an overall conclusion. As the data and analysis later show, some of the criteria suggest stronger confidence in a declining trend while others suggest skepticism and doubt. Furthermore, three of the six remaining criteria, *responsibility*, *measurability*, and *presumptive legitimacy,* are also weighed slightly more heavily than the others. For the purpose of this thesis, these three are more applicable for the analysis. *Responsibility* addresses trends in identifying China as the perpetrator of an attack, which can translate to confidence in the data itself. Similarly, *measurability* addresses trends in how well companies can identify damages, which also translates to the degree of confidence in the data. Last, *presumptive legitimacy* addresses whether the attack was on a civilian or government organization. Since the Agreement differentiates civilian companies as

unacceptable targets and government companies as potentially legitimate, a change in Chinese attacks toward either also changes the overall assessment.

In comparison, the other three criteria, immediacy, directness, and invasiveness, play a lesser role in applicability. There is a lack of information due to this author's lack of technical knowledge of the author and a lack of data on the attacks themselves. None of the reports provide an in-depth timeline and given the nature of cyberspace operations, identifying when and for how long a cyberattack went on for is shaky at best. Additionally, much of the technical details are difficult to transcribe into measures of directness and invasiveness. Little, if any, of the framework provides a means to translate methods of attack into a measure of either criterion.

4. Limitations

During research and assigning values for each attack, this author discovered several limitations in analysis. First, although the purpose of quantifying the data is to create a more objective approach toward analysis of cyberattacks, in practice, the assigned values are still fairly subjective. As a result, Appendix B contains the raw data used to produce the graphs, which, as will be covered Chapter V, can be used for future research. *Presumptive legitimacy*, for example, is relatively subjective considering attacks on both private and public sector. An attack on 10 total targets, 7 governmental systems and 3 civilian systems, versus an attack on 20 total targets, 14 government and 6 civilian, has the same ratio, but ratio is not necessarily the best measure. There are far more civilian companies than governmental agencies, thus it is potentially more accurate to weigh attacks on government systems more heavily.

Second, each of the criteria consists of several subset criteria, thereby potentially generating a bias in observation. Considering *severity,* while this thesis measures economic damages, the value does not necessarily reflect economic gain for China. Stolen emails and data does not mean China succeeded in improving their position, nor does the theft of military information necessitate a gain in technological capacity. Data from the F-35 program could have been used to generate counter-tactics, rather than furthering China's aviation program.

Lastly, the data gathered is inherently skewered toward known and/or reported attacks. As a result, it is possible that there are far more attacks by Chinese actors than the ones listed, especially considering there is often a delay in discovery of a cyber intrusion. Furthermore, given the complexities and politics of classified and confidential information as well as a myriad of factors that make reporting of cyber intrusions undesirable, it is likely there are more incidents than ones analyzed in this thesis.

D. RESULTS AND ANALYSIS

Overall, the findings in every category were fairly sporadic. Under all seven criteria, there did appear to be a discernable pattern of activity. The results ultimately suggest that Chinese cyberattacks have either remained unchanged over time or declined in a way that is favorable from a U.S. standpoint. This section describes the findings for each of the criteria and analyzes of the data, providing possible insight as to what conclusions one may draw from such results. Additionally, each explanation also discusses pitfalls in using this methodology and identifies possible areas of improvement for future research.

1. Severity

This section depicts two graphs. The valuation for the severity of attacks can be seen in Figures 15 and 16. Total damage inflicted is reflected in Figure 15 whereas economic impact is displayed in Figure 16. Additionally, like Chapter III, this section displays linear trend lines and their associated function and R-squared values.

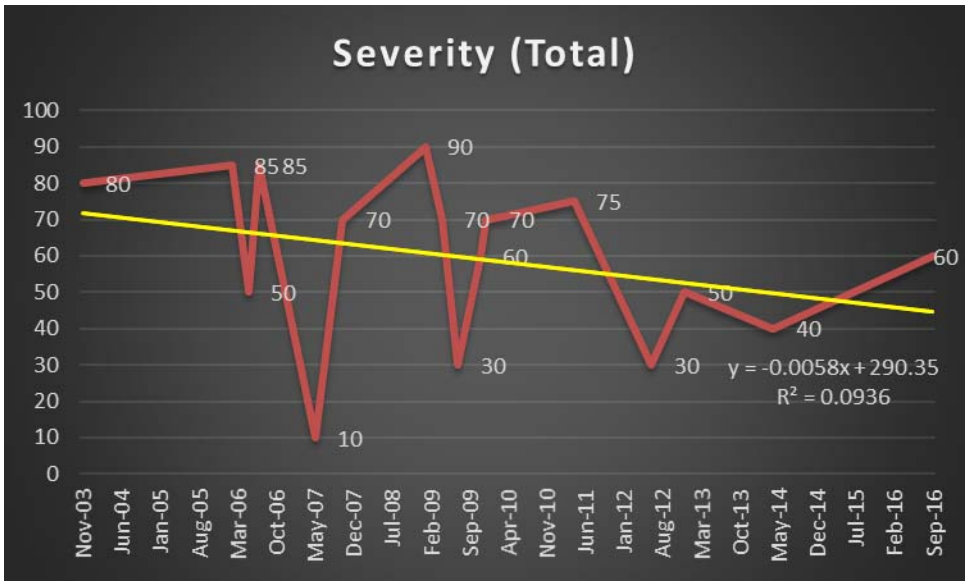


Figure 15. Severity (Total) from Date of Earliest Indication[205]

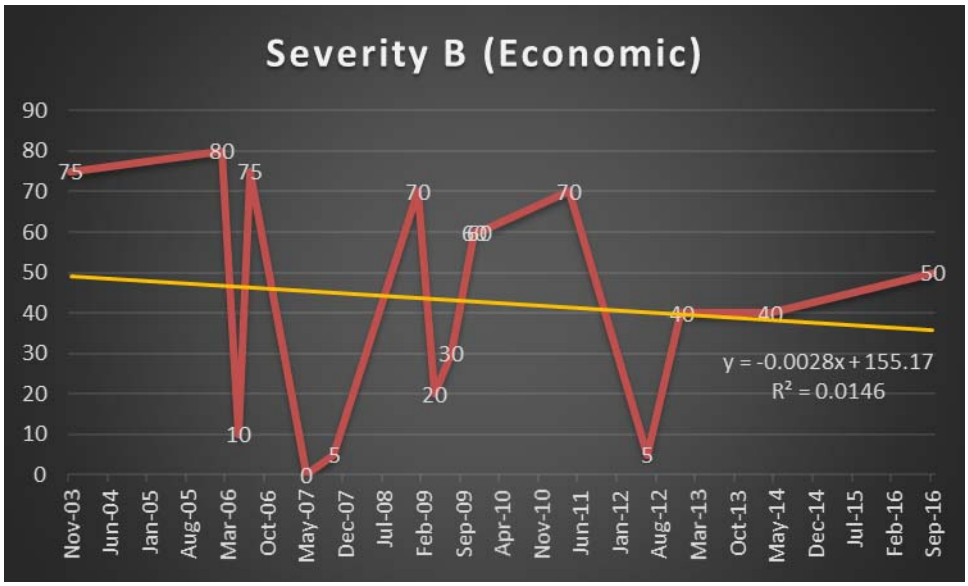


Figure 16. Severity (Economic) from Date of Earliest Indication.[206]

In Figures 15 and 16, the data suggests that the dominant opinion is correct: the Agreement has made no major impact. Instead, the decline in attacks, or in this case,

[205] Note: Data was derived from multiple sources. See Appendix B for details.

[206] Note: Data was derived from multiple sources. See Appendix B for details.

severity, is a change taking place over a number of years, which one can see from the trend lines. Figures 15 and 16 show a slope function of

$$y = -0.0058x + 290.35$$

and

$$y = -0.0028x + 155.17$$

Both equations possess negative *m*-values, suggesting *severity*, in either case, is declining. While neither value is particularly large, their values do suggest a trend to U.S.-China cyber relations.

This decline in the *severity* of attacks, while slow, is a step in the right direction from a U.S. standpoint. If this trend persists, the possibilities for more areas of mutual understanding and cooperation like the Agreement are likely to increase. Therefore, although far from a foregone conclusion, the Agreement may potentially become akin to the 1972 Communique, a moment in bilateral relations aiding to the actual normalization of relations between the United States and China. Furthermore, because the *severity* of attacks is not rising, the trend contradicts the counter-argument that China is adopting a Russian model. If, as analysts like Mr. Costello suggested, Chinese policies were adopting the Russian model, one would expect to see a rise in *severity.* More sophisticated and targeted attacks, theoretically, should cause more damage. Expectations would include theft of multiple programs or intellectual property such as blueprints for Apple's iPhone. The data, instead, shows not only fewer instances, but also fewer indications of intellectual property actually being siphoned off.

Overall, the data from *severity* appears promising. There is a decline and, more importantly, there is not a rise in attacks. Thus, should conditions hold, it seems prudent to push for additional cooperation. Despite such promise, however, there are limitations in the data, particularly the slow rate of change and the relative lack of information means the United States should move forward cautiously in U.S.-China cyber relations.

The slow rate of change is concerning because of how quickly the results may become irrelevant. If, for example, there is a drop from 50 to 40 (-10) over the span of

one year, but a rise from 40 to 80 (+40) in the following year, then small initial drop may mean very little. Therefore, although there has been a decline in *severity* over the past decade, one bad year can quickly reverse the trend. If, instead, the decline was much larger, then reversing the trend would be much more difficult. For instance, a drop from 100 to 50 (-50) in one year and a rise from 50 to 90 (+40) the following year is still an overall decline. As a result, assurances from one government to the other can remain fairly robust, even if there is a surge from unsanctioned hackers. Although such numbers do not preclude cooperative efforts, the small rate of change will likely elicit, with good reason, caution from the U.S. side.

Also eliciting some caution from the results is the relative lack of information on the attacks. As many of the following sections also discuss, the reports generally lack information vital for the determining specific Chinese behavior in cyberspace. In the case of *severity,* none of the reporting data specified what was stolen or listed specific damages from the intrusion. Analysts report that data relating to a specific program or piece of intellectual property was stolen, but they do not specify what the data is exactly. Moreover and related to the data, analysts do not provide any dollar estimates of damages caused by the attacks.

In sum, the data on *severity* is promising, but not concrete enough for the United States to presume Chinese behavior has completely changed. As is discussed later, such results will likely come to play a much larger role as talks and further agreements continue between the United States and China.

2. Immediacy, Directness, and Responsibility

Valuations for *immediacy*, *directness*, and *responsibility* are reflected in Figures 17, 18, and 19.

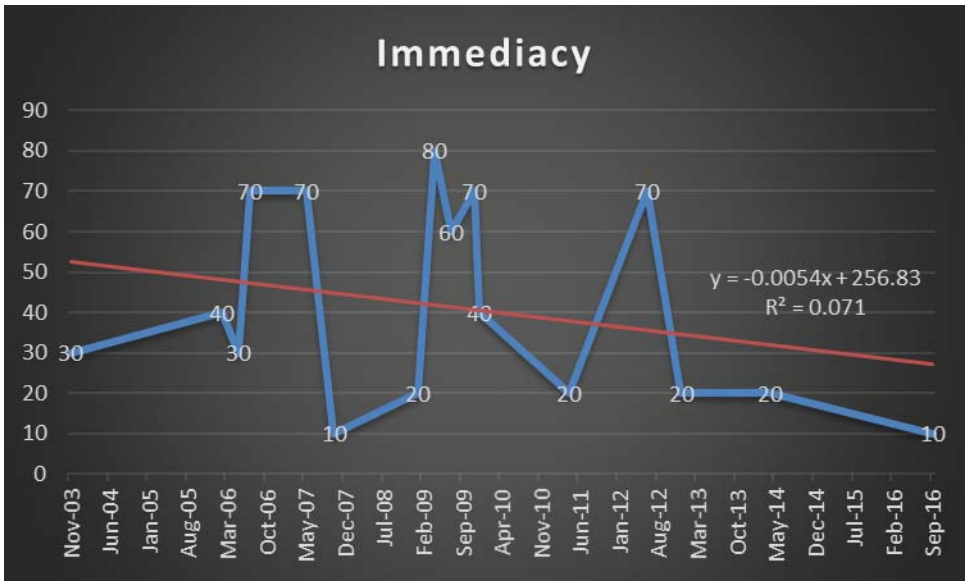


Figure 17. Immediacy[207]

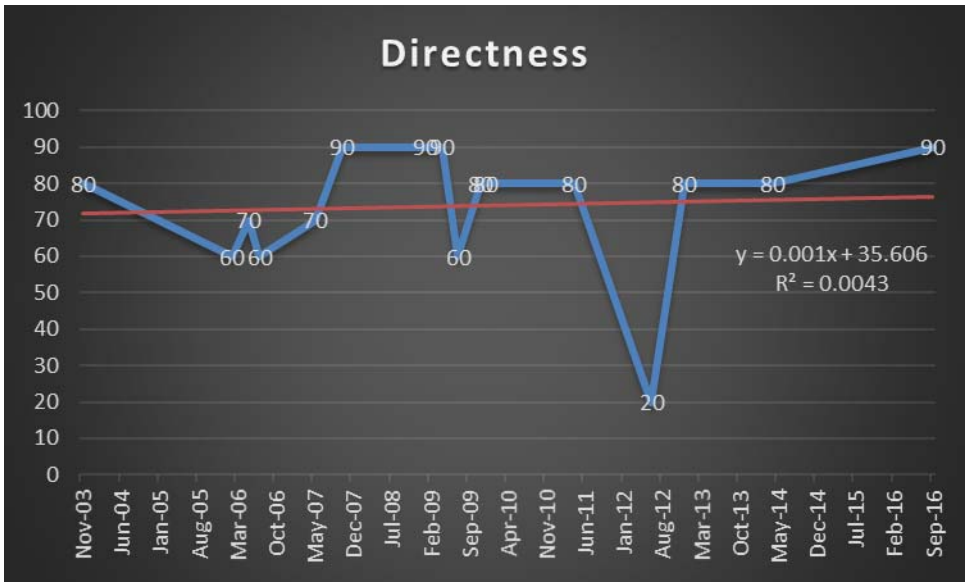


Figure 18. Directness[208]

[207] Note: Data was derived from multiple sources. See Appendix B for details.

[208] Note: Data was derived from multiple sources. See Appendix B for details.

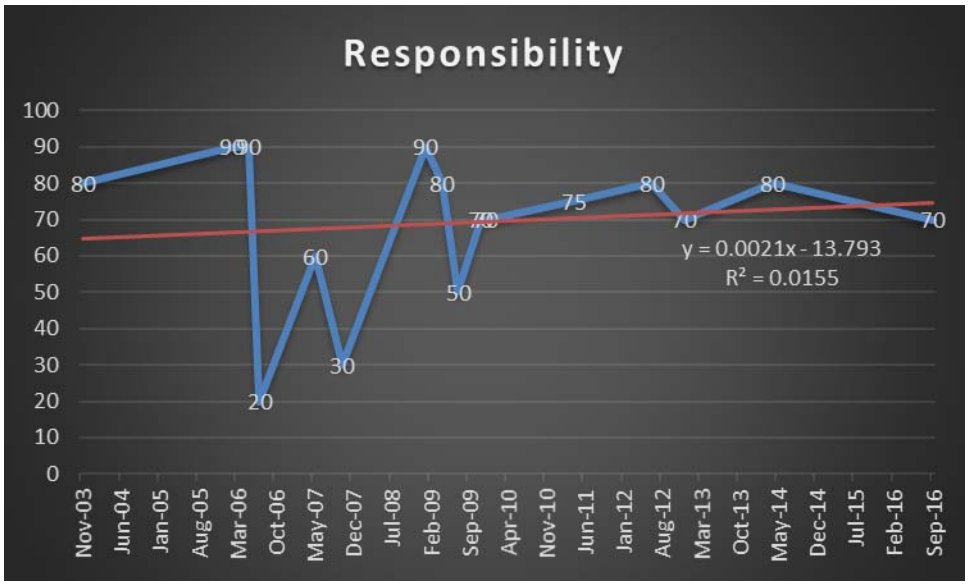


Figure 19. Responsibility[209]

The data in Figures 17, 18, and 19, shown above, also suggests that there is a promising trend in Chinese behavior. In Figure 17, the values were assigned based on two criteria: the timeline between intrusion and attack and the overall length of intrusion. This author assigned higher values if the timeline and length of intrusion were rising, and lower values if the reverse. The result being a slope equation of:

$$y = -0.0054x + 256.83$$

Again, there is a negative *m*-value indicating the trend is falling. The data, thus, suggests attacks are occurring closer to the initial intrusion and that the overall length of intrusion is decreasing.

Figure 18, similarly, suggests there is a rising trend in cause and effect. The *m*-value in this case is positive with a slope equation of:

$$y = 0.001x + 35.606$$

The value, although small, indicates that Chinese attacks are more goal-oriented than targets of opportunity. *Shady Rat*, for example, attacked multiple companies in the

[209] Note: Data was derived from multiple sources. See Appendix B for details.

same industry, suggesting the attackers' strategy was to gain information where available. Problems of this strategy are that there is much more opportunity to discover the attacks and that efforts are often duplicated. Since, however, Figure 18 shows a positive value, the data suggests attacks are more focused and targeted.

Lastly, Figure 19 suggests that analysts are growing better at tying attacks to Chinese actors. The positive *m*-value, in this case, shows there is a rising trend at attributing cyberattacks to Chinese actors. Comparing the information on "Wicked Rose" and the indictments of Su Bin and APT1, for example, highlight analysts growing capabilities at attributing China as the perpetrator with more substantial proof.[210] Ken Dunham and Jim Melnick identified Tan Dailin as the leader of Wicked Rose in 2006.[211] Analysts tied him to the attacks by identifying his social media profile, tracing his location back to China, and establishing his ties to the CCP.[212] While the evidence is fairly strong, much of the data is still circumstantial. The indictments, in comparison, are much more compelling. The documents list exact dates on when particular portions of the operation were launched, including when email addresses were created, when files were sent, and where data was hosted.[213] The evidence makes it far more difficult for the actors to deny their involvement and, as a result, are much more damaging for China's image internationally.

These findings suggest that there is some change in Chinese behavior. Chinese actors appear to be attacking more directly. Rather than infiltrating a network, monitoring traffic, and then waiting to siphon information, infiltration and theft seem to occur in a much faster sequence. One explanation in this shift is that attackers' efforts are better

---

[210] Ken Dunham and Jim Melnick, "'Wicked Rose' and the NCPH Hacking Group," Krebs on Security, November 2011, http://krebsonsecurity.com/wp-content/uploads/2012/11/WickedRose_andNCPH.pdf.

[211] Ibid.

[212] Ibid.

[213] United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, Criminal No. 14–118, U.S. District Court, Western District of Pennsylvania, May 1, 2014, https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf; United States of America v. Su Bin, Docket No. 14–1318M, U.S. District Court, Central District of California, June 27, 2014, https://www.theglobeandmail.com/news/national/article19704622.ece/BINARY/Su+Bin+1030+complaint.pdf.

targeted. As time progresses, Chinese policy, as will be explored in greater detail in the following chapter, may be shifting from the "death by a thousand cuts" toward precision guided attacks.[214] Attackers, whom previously infiltrated networks to monitor traffic in hopes of finding information, may now have preassigned data to steal.

There are also many alternative explanations for this shift in behavior. Rising technological innovation and improved techniques, for example, suggest change could be expected. Discovery of new zero day exploits and an increase in infrastructure capacity to transfer data allow for much faster attacks. As a result, terabytes of data can be stolen in the matter of seconds rather than minutes.

Of course, there are many counters to both explanations. As discussed earlier, there is an apparent lack of data. Many of the reports do specify the length of intrusion, but none of the reports describe their confidence level in their assessments. It is possible intrusions occurred over a larger period of time, but were undiscovered. Additionally, the reports focus on the offensive elements of the attacks, ignoring any discussion of defensive capabilities. Therefore, there is some uncertainty in the reliability of the conclusions.

Despite the unreliability, however, the data are indicative. If intrusion lengths are falling and better targeted, and Chinese behavior has shifted, this alters part of the previous conjectures. A drop in the volume of attacks and more targeted efforts do suggest a change toward the Russian model; however, the drop in severity suggests that may be a good thing. Fewer attacks, albeit more targeted and sophisticated, coupled with less severity, together mean less damage overall. This suggests reversal of the rising trend of "the greatest transfer of wealth in human history," or at the very least that the situation is not getting worse.[215]

---

214 Jon R. Lindsay, "The Impact of China on Cyber Security: Fiction and Friction," *International Security* 39, no. 3 (Winter 2014/15): 7–47, https://doi.org/10.1162/ISEC_a_00189.

215 Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" Foreign Policy, July 9, 2012, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

3. Invasiveness

Valuation for *invasiveness* is reflected in Figure 20.

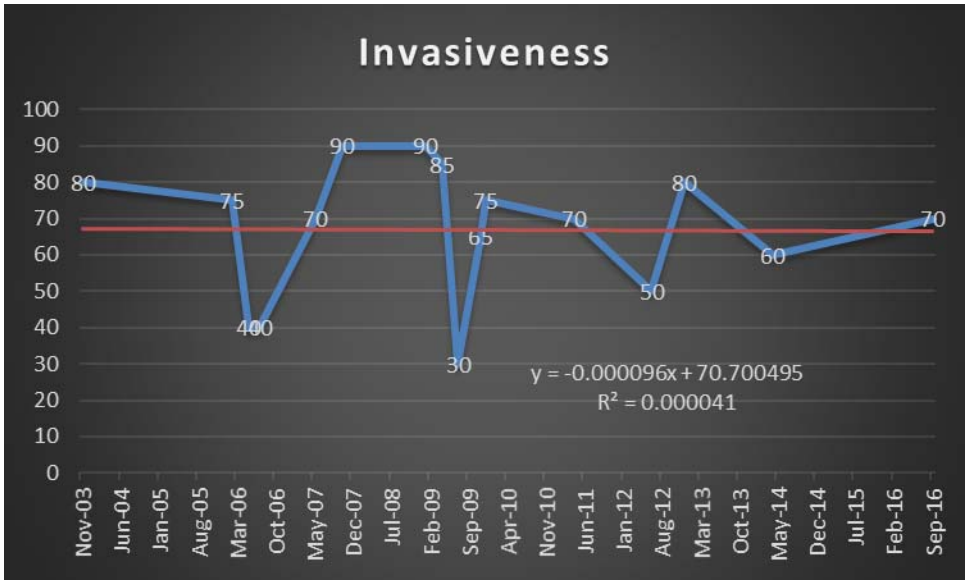


Figure 20. Invasiveness[216]

The results from invasiveness suggest there is almost no change in Chinese behavior. The slope equation from the data is:

$$y = -0.000096x + 70.700495$$

The *m*-value, in this case, is relatively negligible. The value from *directness,* for comparison, was 0.001 and was the smallest *m*-value outside of *invasiveness.* Even so, the value from *directness* is over 100 times greater than the *m-value* here. This value suggests that overall Chinese attacks continue to intrude into networks unchanged, varying between U.S. and non-US networks, but generally operating intrusively onto U.S. infrastructure.

Since attacks generally occur on U.S. networks, this thesis can infer a couple conclusions on Chinese behavior. First, despite any rhetoric criticizing China, attacks are

216 Note: Data was derived from multiple sources. See Appendix B for details.

likely to focus their efforts on U.S. networks. Likely due to security policies governing that intellectual property be kept on U.S. infrastructure, attacks seem unlikely to shift their focus to theft on Chinese servers. Second, attacks appear limited toward exploits over networks rather than hardware exploits. None of the attacks, thus far, have used hardware as part of their methodology. If, for example, attackers began to use embedded hardware to sniff and steal data, the baseline for *invasiveness* would likely increase as attacks would become far more intrusive. Therefore, this thesis can conclude, for now, cyberattacks are unlikely to delve into the physical realm.

4. Measurability

Valuation for *measurability* is reflected in Figure 21.

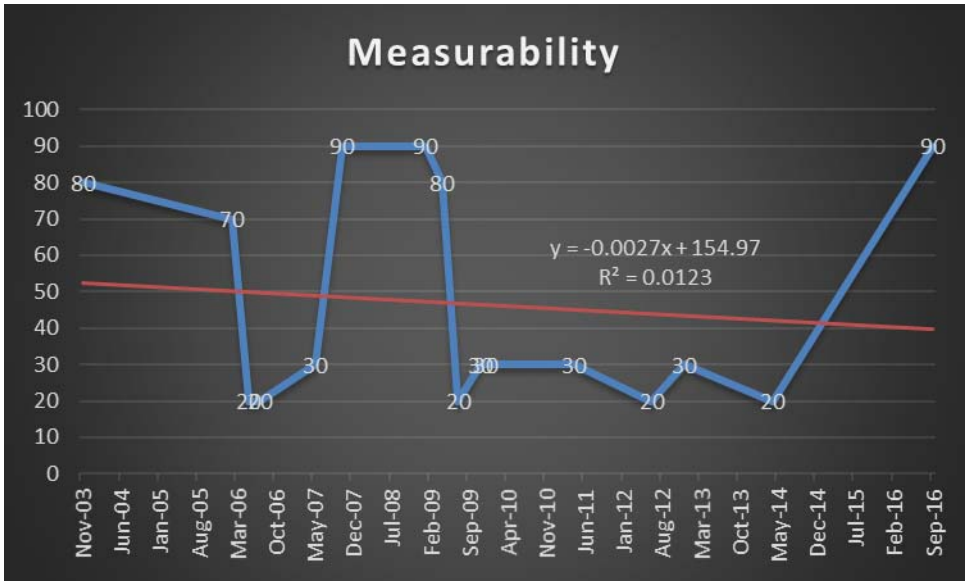


Figure 21. Measurability[217]

The results in measurability show a declining trend in the ability to evaluate damages. As time progresses, it is increasingly more difficult to assess the damages caused by a cyberattack. Although a relatively small m-value, the value is still negative with a slope equation of:

217 Note: Data was derived from multiple sources. See Appendix B for details.

$$y = -0.0027x + 154.97$$

The negative value indicates that the damage from an attack is becoming harder to evaluate. Either reports are becoming less focused on discussing the damages caused by an attack, or there is less information on the damages. The first explanation is amendable. Without diving into the realm of shareholders and incentives for a company to do so, analysts and companies can do a better job on reporting the damages inflicted by a cyberattack.

In the case of the latter explanation, however, the trend complicates the ability to provide an accurate analysis. If companies simply do not know what was stolen, then all of the previous conclusions may be wrong. Given previously discussed presumptions that Chinese hackers are caught and identified more frequently, and therefore are less sophisticated and less worrisome than Russian hackers, then a reverse of this position means reformulating all analysis based on those assumptions. If, alternatively, Chinese attacks have advanced now to the point where the information stolen is unknown, the data would suggest their level of sophistication is rising to a point beyond prior assessments. The evaluation under s*everity,* then, may underestimate the damage of cyberattacks. If, instead, *severity* is rising, the data would then suggest the shift in Chinese behavior is more worrisome, not less.

5. Presumptive Legitimacy

Another problematic shift in Chinese behavior is reflected in Figure 22.

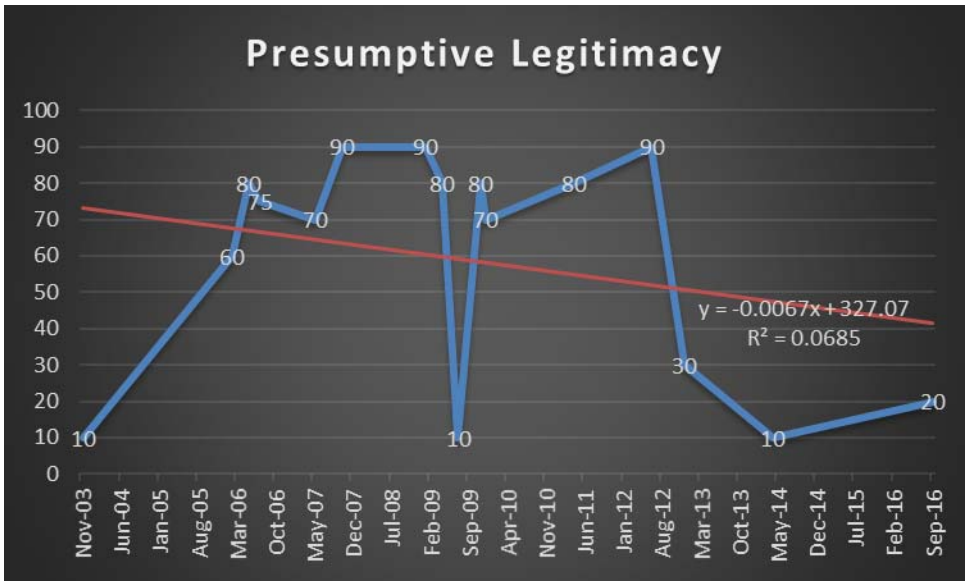


Figure 22. Presumptive Legitimacy[218]

Again, represented by the negative *m*-value, the graph suggests attacks are moving toward civilian rather military or government targets. As the Agreement specifically stipulated that neither side would engage in economic theft, thereby inferring a difference from military and government targets, one would hope behavior would change away from civilian targets. Instead, however, attacks appear to move toward only civilian targets.

This trend is particularly alarming considering overall Chinese behavior. If China's methodology is moving toward the Russian model, then the drop in attacks and *severity* may primarily come from a shift away from government and military targets. Therefore, the Agreement and promising trend in Chinese behavior may mean far less than previously discussed.

E. PROSPECTIVE ALTERNATIVES

Since this analysis is built upon a subjective perception of the criteria and data, there exist several other methods of interpreting and evaluating the data. This section discusses some of the possible alternatives, particularly those generating results that

218 Note: Data was derived from multiple sources. See Appendix B for details.

differ substantially from the results presented in Section D. Additionally, Appendix C provides the raw data used to create the graphs in this section to again allow for future research and evaluation.

1. Severity

Recalling, briefly, that one of the main purposes of the Agreement is to stem economically motivated cyber espionage, a way to measure *severity* and the successfulness of the Agreement is to track potential gains. Rather than economic damage, tracking economic gains potentially offers a way to assess whether there is a change in thresholds for cyberattack. If, for example, cyberattacks shift toward attacking only high reward targets and cease attacking low reward targets, then one can infer that there is a change in China's risk calculations. Given, however, the relative lack of information regarding intellectual property, much of the analysis is speculative. It is not reported or otherwise not known what information was potentially compromised or actually stolen. The analysis, therefore, assigned values from zero to two, with zero being no commercial value, one as low value, and two as high value. The measurement of *severity* is depicted in Figure 23.

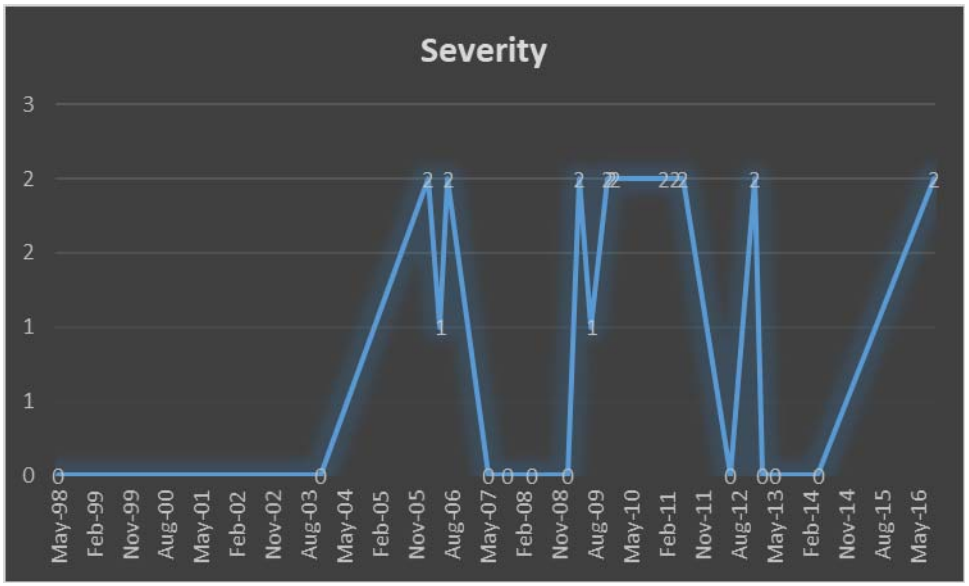


Figure 23. *Severity*[219]

No apparent pattern is discernible in Figure 23. While there is a distinctly short sample size of data following the Agreement, the data thus far does not indicate a preference for high value commercial targets. Instead, attacks are varied between "legitimate" targets and private enterprises. Thus, looking at the data this way, Chinese behavior may remain unchanged in terms of target selection, thereby also discounting the findings in *presumptive legitimacy.*

If Chinese behavior remains unchanged, however, then the earlier interpretation that *severity* is decreasing may be more promising for the United States. Since the target list is not shifting toward military targets, the declining trend likely includes commercial targets. More simply put, damage inflicted by Chinese attacks on commercial companies apparently has fallen.

2. Invasiveness

Another alternative perspective concerns the concept of *invasiveness*. Instead of defining *invasiveness* as sovereign territory of a state, one can instead define it in terms akin to the Open Systems Interconnection (OSI) model. To provide a brief summary, the

219 Note: Data was derived from multiple sources. See Appendix B for details.

OSI model is a conceptual framework of how data is communicated over a network. The framework is split into seven layers, shown in Figure 24.

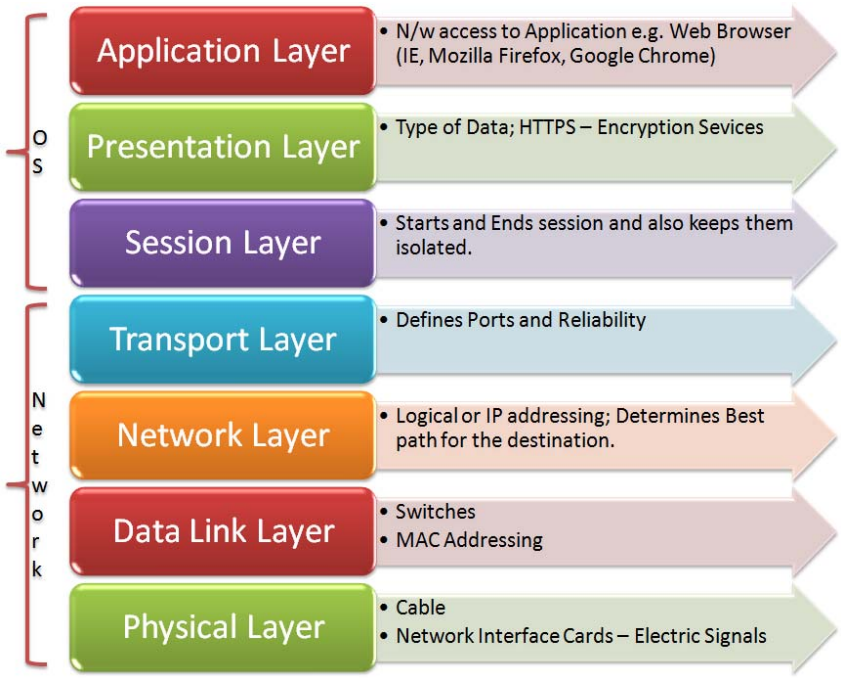


Figure 24. OSI Layers[220]

The seven layers designate different locations at which data can exist. For the purpose of the present analysis, in regards to *invasiveness*, this translates to differing depths of penetration. Taking the perspective of the target system, the layers can be perceived as levels of *invasiveness* from one to seven with one, the physical layer, as the least invasive and seven as the most invasive. Consequently, this author's measurement of *invasiveness* is provided in Figure 25.

220 Sue Giles, "OSI Model," Tes Teach, accessed November 9, 2017, https://www.tes.com/lessons/AMRvJVl32tmEEQ/osi-model.

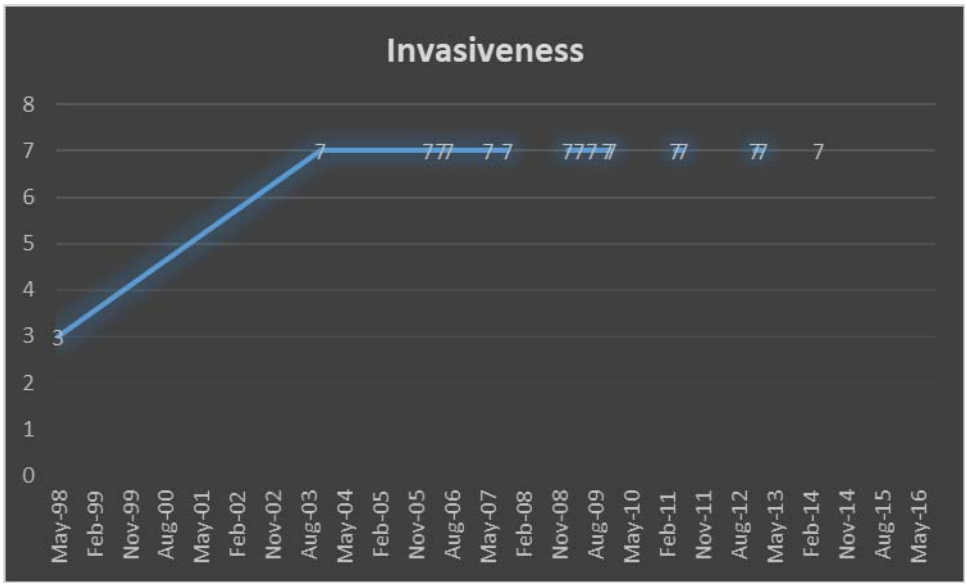


Figure 25. *Invasiveness*[221]

The data shows that intrusions routinely and consistently reached the application layer. Though many of the attacks started via phishing attacks, the theft ultimately occurred directly through client-based applications. In terms of a physical domain analogy, attackers routinely stole directly from the victim's home instead of stealing packages from the front door.

While alarming, however, the results may suggest a major flaw in the data. As the idiom goes, the squeaky wheel gets the grease. Reports of Chinese cyber intrusions are inherently biased toward those that succeed. In other words, reports do not generally cover failed attempts. Given the fact that attacks use the same infrastructure and medium as legitimate traffic, it is difficult to differentiate the signals, attacks, from the noise, routine. Furthermore, as many of the reports suggests, cyberattacks occur frequently and often, but systems are designed to stop them before they have a chance to succeed. Thus, the data likely omits many failed attempts by Chinese actors. As a result, there is a degree of uncertainty in the confidence of the overall trends.

221 Note: Data was derived from multiple sources. See Appendix B for details.

3. Other Prospects

Though neither of the alternate perspectives completely discredits the overall findings in Section D, they do highlight the possibility and potential of contradictory results. Furthermore, as additional information on existing attacks and new attacks comes out, the findings and alternate perspectives must also adjust. Analysis of i*nvasiveness* can be changed to differentiate between stealing and corrupting data. *Responsibility* can be adjusted based on U.S. indictments, providing a scale of the extent the U.S. or U.S. companies are willing to identify the PRC as the perpetrator. In sum, there are many other potential perspectives with which to test the data, reinforcing how the Schmitt Analysis provides additional utility as a framework for analysis.

F. CONCLUSION

Overall, the findings from using the Schmitt Analysis support much of the current dialogue around the Agreement: "cautious optimism."[222] Chinese behavior is changing. The *severity* of attacks is falling; therefore, there appears to be less damage to the United States. Additionally, Chinese methodology appears to be moving away from death by a thousand cuts and lastly, the United States is getting better at tying Chinese actors to the crime. As a result, there is much to be hopeful about.

Yet, the problems under *measurability* and *presumptive legitimacy* may spoil all of those achievements. If attacks are harder to measure and are solely focused on civilian organizations, the Agreement may be doomed. The two sides seemingly established that theft in support of national defense, or in this case cyberattacks on military and government organizations, is acceptable, but attacks on civilian organizations are not. If China, however, entered into the Agreement with false intent, future cooperative efforts may be greatly impacted for the worse. More importantly, if the United States acts too much in good faith and does not challenge and investigate whether China is holding up its end of the bargain, the greatest transfer of wealth might just come to fruition. Thus, the U.S. must proceed with caution.

[222] Kim Zetter, "US and China Reach Historic Agreement on Economic Espionage," Wired, September 25, 2015, https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/.

Lastly, in terms of the Agreement, the results here essentially support FireEye's findings. Rather than a watershed moment, the Agreement appears to be a continuation of change in Chinese behavior. Chinese policy seems to be focusing away from stealing U.S. secrets, perhaps part of an attempt to grow their own domestic innovation. In any case, the Agreement seems to be part of a much larger change.

V. CONCLUSION

Nothing is permanent in this wicked world, not even our troubles.

—Charlie Chaplin

Like any relationship, trends in U.S.-China cyber relations are far from permanent. One good year does not necessarily dictate the results of the following year, especially considering the ever-evolving nature of the cyber domain. As shown in Zhao Weibin's article, "The Four Stages of Sino-American Cyber Relations," the nature of U.S.–China cyber relations can change and have changed rapidly and with little forewarning.[223] For example, Google's withdrawal in 2010 displayed how quickly U.S.–China ties in the private sector can dissolve. In addition, China's withdrawal from the U.S.–China Cyber Working Groups in 2014 amidst U.S. accusations of cyber espionage also showed that public sector ties can dissolve equally fast. Moreover, both cases were preceded by years of cooperative efforts including confidence-building measures, yet still dissolved rapidly.

Still, despite the relatively impermanent nature of a relationship, one can draw clues of how best to go forward to give ourselves the best chance at an optimal outcome. This thesis, as a result, investigated and analyzed the 2015 U.S.-China Cyber Agreement for clues that may aid U.S. decision-makers as to the future outcomes and implications the Agreement has had on the international community and toward shaping norms in cyberspace.

Consequently, this final chapter reviews and summarizes the overall findings from the previous chapters and synthesizes the broader significance in terms of U.S. cyber policy and future research. This chapter is organized as follows. Section A provides a summary of the findings. Section B, then, explains the implication of the results in terms of the model provided in Chapter I. Section C provides policy recommendations based on the results. Last, Section D identifies areas for future research and analysis.

[223] Zhao Weibin, "The Four Stages of Sino-American Cyber Relations," China U.S. Focus, October 9, 2017, https://www.chinausfocus.com/peace-security/the-four-stages-of-sino-american-cyber-relations.

A. SUMMARY OF FINDINGS

Chapter II explored whether the impact of the Agreement would be limited as skeptics like David A. Mussington and Shannon Tiezzi warned or whether the evidence suggested a broader behavior shift on China's part.[224] After review of current evidence from the two years following the Agreement, the results suggest that there is a genuine attempt on the part of the Chinese Communist Party (CCP) to improve U.S.-China cyber relations. Since the Agreement, the CCP made several policy changes that are much closer to U.S. norms. From the development of intellectual property rights to establishing additional international cyber agreements with other countries, the CCP's efforts seem to be sincere. More importantly, U.S.-China cyber relations are better than they have ever been.

In Chapter III, this thesis explored the data surrounding the volume of attacks and found that the Agreement likely played a part toward improving U.S.-China cyber relations. While the data supports FireEye's assessment that the Agreement was not a watershed moment, it did act as an accelerant, speeding the rate of change. Additionally, in terms of global cyberattacks, Hackmageddon's data supports that finding: there is little other explanation as to why the rate of drops increases in 2016, given 2016's absence of punitive actions. Lastly, trends of rising capabilities in cybersecurity and lack of evidence for improving Chinese cyber techniques suggest that fears of China moving toward a Russian model are unwarranted. Thus, overall, Chapter III's analysis of the data suggests, from a U.S. standpoint, a more promising relationship.

While that is promising, judging cyber-relations by volume alone leaves significant gaps in knowledge. Going beyond the general reliance on the volume of attacks as the sole metric on which to judge the effectiveness of the Agreement, Chapter IV repurposed the Schmitt Analysis as an alternative model to weigh the Agreement. Using Schmitt's seven criteria, this thesis evaluated Chinese cyberattacks and found

---

[224] B. David A. Mussington, "The Missing Compliance Framework in the 2015 U.S.-China Cybersecurity Agreement," Institute for Defense Analysis, November 18, 2015, https://www.ida.org/~/media/Corporate/Files/Publications/IDA_Documents/ITSD/2015/D-5648.ashx; Shannon Tiezzi, "The Limits of a US-China Cyber Deal," *The Diplomat*, September 22, 2015, https://thediplomat.com/2015/09/the-limits-of-a-us-china-cyber-deal/.

similar results to Chapter III: Chinese behavior is changing in a way that is more beneficial for the United States. China is shifting toward less damaging attacks, and U.S. ability to accurately and confidently attribute attacks, with particular regards to Chinese actors, is improving.

Overall, in the two years since the Agreement, the evidence suggests hope for a better, more promising U.S.-China cyber relationship. Not only are there fewer attacks, but the two are also strengthening ties by expanding bilateral institutions that help insulate cooperative efforts from short term developments like changing presidents or minor conflicts. In the end, actions are following words; thus, although the United States must act cautiously, there is reason for hope.

B. HYPOTHESIS ASSESSMENT

The conceptual design of this thesis aimed to examine the impact of the Agreement on U.S.-China cyber relations by exploring four possible outcomes as shown in Figure 26.

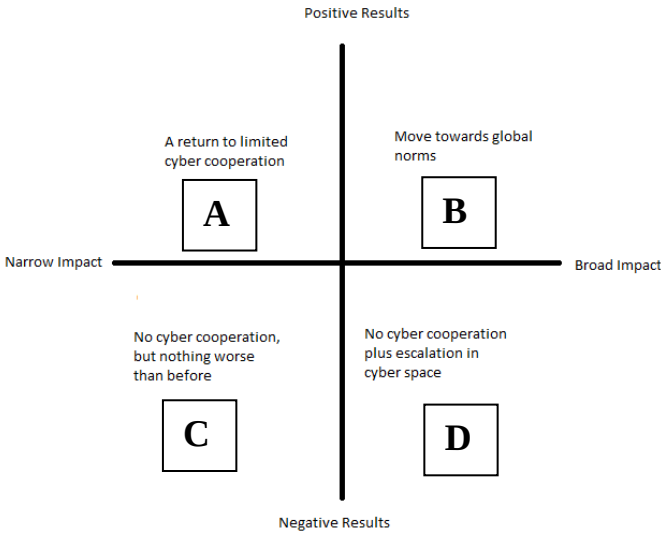


Figure 26. Possible Outcomes

Ultimately, the results of this thesis found that the impact fell into quadrant B, a move toward global norms. The data strongly suggests positive results; not only is there a drop in the volume of attacks, but indications are that China is not moving toward a Russian model. Additionally, given the changes in Chinese policy, the evidence suggests the Agreement made a broader impact in U.S.-China cyber relations as the two are acting more cooperatively than ever and China is expanding similar engagement globally. These developments are likely to positively influence the development of global cyber norms.

Prior to the Agreement, the two sides' perception of cyberspace vastly differed. General sentiment in the United States perceived China as the clear cyber aggressor, causing deliberate harm to the U.S. economy and security. From a Chinese perceptive, however, U.S. accusations were ridiculous and just a means to draw attention away from similar U.S. actions. As a result, U.S.-China cyber relations seemed doomed because policymakers would be fated to talk around one another.

Following the Agreement, however, with perspectives more closely aligned, which makes establishing global cyber norms much more feasible. Starting in 1998, the United Nations Group of Government Experts (GGE) "began considering issues of cybersecurity."[225] Since then, the panel discussed the topic of establishing global cyber norms multiple times though they failed to find common ground. Although talks also failed in their most recent attempt in June of 2017, it appears as though China was a much more active participant.[226] Given that, in the past, China has generally been a passive participant, their new role suggests hope from a U.S. standpoint. With the changes described in this thesis, establishing a global taboo on economically motivated cyber espionage seems more likely, especially considering the numerous bilateral agreements between China and other states being formed today. Such future progress would be a tangible indicator that trends identified in this thesis are continuing.

---

225 Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," Hoover Institution, *Aegis Paper Series* no. 1703, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.

226 Adam Segal, "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?," Council on Foreign Relations, June 29, 2017, https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

Recognizably, however, many of the previous criticisms of the Agreement remain true. There is no consensus on "what the United States and China would constitute as an economic target," nor does the Agreement specify any consequences should either side violate the terms.[227] Furthermore, with the growth of the Internet of Things and other major technological and societal developments, the U.S.-China cyber relationship could essentially change overnight. Therefore, both parties need to take caution moving forward.

On the U.S. side, relying on a decline of Chinese cyber espionage could still feasible play into a malicious Chinese strategy. Much like nuclear strategy conversations, policies that commit the United States to act a certain way based on faulty assumptions are dangerous. For example, some critics argue the nuclear deal with Iran plays into Iranian strategy of biding time until Iran's economic strength is sufficient to continue a nuclear program. In that case, the United States is acting on a faulty assumption of how much Iran values a role as an active participant in the global community. China is potentially playing a similar role. If so, the 2015 Agreement is simply a way to stall for time until China is better equipped and ready to use cyber espionage to its benefit.

Still, the evidence suggests many of the skeptics are wrong to be pessimistic. The Agreement does not appear to be "purely 'symbolic'" and, more importantly, it has not been "unfeasible for China to uphold."[228] Especially considering Chinese policy developments, many of the skeptics seem to underestimate the CCP and overly pursue China as an enemy. As a result, viewing the CCP only a cyber adversary risks missing an opportunity for further strengthening of these nascent cooperative achievements.

C. POLICY RECOMMENDATIONS

Given the results of the Agreement examined in Chapters II, III, and IV, this thesis argues that U.S. policy should progress toward expanding U.S.–China cyber

---

227 Jamie Ellis, "Chinese Cyber Espionage: A Complementary Method to Aid PLA Modernization," (master's thesis, Naval Postgraduate School, 2015), https://calhoun.nps.edu/bitstream/handle/10945/47941/15Dec_Ellis_Jamie.pdf?sequence=1&isAllowed=y, 116.

228 Ellis, "Chinese Cyber Espionage," 116.

cooperation. Additionally, the changing security environment coupled with the ever increasing development of technological innovations suggest an increasing level of futility in the reliance on punitive actions and defensive measures as a means to stop or even limit the rising costs of cyber espionage. As a result, a combination of the cooperation and defense is necessary to solving the problem of economically motivated cyber espionage between the two nations.

1. Preventing the Proliferation of Cyber Espionage

Since damages of cyber espionage continue to grow at an alarming rate, a critical element of U.S. policy must work to solve that problem. Especially given more bilateral talks with China, the two cyber superpowers are in a unique position to work together toward discouraging commercial cyber espionage more broadly.

First, with both nations' history of using a myriad of cyber tools, techniques, and procedures to pilfer intellectual property, the two have a distinct advantage in patching security vulnerabilities. One of the major problems in cyber defense is simply knowing what to defend. As previously discussed, one of the more complicated techniques is the utilization of zero-day exploits. Thus, sharing knowledge of exploits and how to patch them can be a cornerstone of preventing and limiting the effectiveness of lower-tier hacker groups, like script kiddies. To that effect, policy should work toward establishing more bilateral ties and talks, particularly among organizations below the strategic level like the FBI, CIA, and so on. The possibility of sharing information, however, is limited by cyber realities. The nature of exploits make them an asset both offensively and defensively. Knowledge of a security vulnerability gives an attacker another avenue for penetration and gives a defender the location of the path needing to be blocked. Coupled with the fact that incentives to steal intellectual property are only growing larger, the degree of knowledge sharing will likely be limited.

Second, bilateral ties and cooperative efforts can increase the effectiveness of punitive measures. Given the global nature of cyberattacks and the reality of perpetrators often living outside of a single nation's jurisdictional boundaries, U.S. and Chinese efforts toward establishing global norms and international laws are key to

nonproliferation. Both nations are establishing more and more bilateral cyber agreements. As a result, not only are the odds of creating global cyber norms rising, but emergence of a network of smaller scale agreements offers a promising future for punishing criminals outside of state's jurisdiction. The United States and China can potentially work as the middlemen to punish a malicious cyber actor, even among other nations with less than desirable bilateral relations like India and Pakistan.

Last, like the early stages of the many trade agreements, the 2015 U.S.–China Cyber Agreement can be strengthened in several ways. First and foremost, the two sides need to insulate the Agreement from rapid changes in the political environment. As an informal agreement between President Obama and President Xi, the Agreement is not protected by ratification by each nation's respective legislation. Second and related to the first, verification and punitive measures need to be established. The two sides need to consider defining the parameters of what breaking the Agreement means and, in the event that one violates the Agreement, how to punish the offending state. As in the case of trade agreements, there is a lack of incentive for either state to forego cyber espionage if the other is not as well, yet neither state is particularly better off in continuing cyber theft activities; thus, leaving both states with a situation akin to the tragedy of the commons. Therefore, international agreements and constraints can work to solve the problem by changing the incentive structure into a more beneficial outcome for both.

2. Sustaining a Safe and Secure Environment

Although diplomatic efforts and establishing greater bilateral ties with China is critical in solving the cyber problem, U.S. domestic policies must also work toward establishing a better cyber environment. While this thesis did not discuss U.S. efforts in depth, Chapter III briefly touched on the subject of improving defensive capabilities. Certainly, the debate over anonymity in cyberspace continues to be a major issue, particularly as one of the key ideological divides between the United States and China. What level of anonymity should users expect? What is the government's role in ensuring that aspect? However, despite the controversial aspects of anonymity and other related

debates, there are still a few ways that the United States can work toward improving the cyber environment.

Technological advancements in securing transmissions have greatly improved reliability and safety of using cyberspace. The development of Hypertext Transfer Protocol (HTTP) with Transport Layer Security (TLS), or HTTPS, vastly improved how secure Internet functions can be. For example, older malicious techniques like website spoofing are much less viable. Browsers inform the user that a site may not be legitimate. Additionally, higher tier encryption methods like SHA-256 over DES help mitigate the problem of brute force hacking, especially considering parallel developments in processing power. Thus, although technological advancements improve malicious actor capabilities, cyber defenses grow as well.

While artificially generating innovation and other elements of total factor productivity (TFP) is not necessarily possible, or reliable, through changes in U.S. policy, policy can impact adherence and implementation of improved security methods. As discussed by proponents of free market theory, government regulations are often inefficient as an artificial means to control market behavior. As Donald Real's article, "Saving Fisheries with Free Markets," showed, however, government regulation can fix problems where the free market produces perverse results.[229] Generally, most companies face little incentive to improve cyber security measures until it is too late. The recent Equifax breach at the end of 2017 is the latest example of the lack of incentive to fix major security gaps. Although specific details have yet to be released, early reports by Matt Tait and Brian Krebs suggest a conscious decision to ignore potential security gaps which are largely unchecked by government regulations.[230] Hence, U.S. policies can go a long way to simply ensuring security in cyberspace.

---

[229] Donald Leal, "Saving Fisheries with Free Markets," *The Milken Institute Review* 57, no. 1 (2006): 56–66.

[230] Matt Tait, Twitter post, 7 September 2017, 10:19 p.m., https://twitter.com/pwnallthethings/status/906024217371525120.; Brian Krebs, "Equifax Breach Response Turns Dumpster Fire," Krebs on Security, September 17, 2017, accessed November 17, 2017, https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/.

3. Future Trajectory of Attacks

A key element of the Agreement's success rests upon the future. The results examined in this thesis cover relatively short-term data. Therefore, it is possible that the result of the Agreement will be a short-term drop, particularly if new U.S. administrations ease off commitments of sanctions and other punitive measures. This thesis, however, argues that possibility is unlikely. Forming the Agreement provides a level of inertia, making a reversal of position on the part of the Chinese more difficult compared to if the Agreement was never formed. Moreover, bilateral mechanisms in place as a result of the Agreement, including law enforcement changes, cannot be easily undone. Although informal, relationships on a first-name basis tend to provide resistance to attempts at completely dissolving ties.

Consequently, the Trump administration, as well as future administrations on both the U.S. and Chinese side, will play a major role in continuing cooperative efforts, but the Agreement has done well to insulate bilateral communication and cooperation from the rigors of short-term politics. U.S.-China cyber relations can still deteriorate, especially if one side discovers disingenuous efforts to undermine the spirit of the Agreement. Even in that case, however, it is more likely the two sides will work together to solve problems if counter-efforts stem from lower level agencies or, if the problem stems from higher levels, unravel and untangle slowly from the cooperative mechanisms in place.

4. Summary

In sum, pursuit of global norms and a better, more cooperative cyber relationship with China, coupled with domestic capabilities, offers a much more promising future. The results of the Agreement suggest working cooperatively with China is producing welcome results. As history has sometimes demonstrated, treating China, or any country, as an enemy may be a self-fulfilling prophecy.[231] Furthermore, working cooperatively produces much greater outcomes than working as adversaries or even just individually.

[231] Joseph S. Nye, Jr, "The Challenge of China," in *How to Make America Safe: New Policies for National Security,* ed. by Stephen Van Evera (Cambridge, MA: The Tobin Project, 2006): 73–77, https://tobinproject.org/sites/tobinproject.org/files/assets/Make_America_Safe_The_Challenge_Of_China.pdf.

As a result, while the United States should continue to monitor Chinese actions, if current results continue, so too should cooperative efforts.

D. AREAS FOR FUTURE RESEARCH AND ANALYSIS

Although this thesis concluded that the results of the Agreement suggest that China is making sincere efforts to improve U.S.-China cyber relations and solve the cyber problem, efforts to monitor the results must continue, for both past and future data.

In terms of past data, including the data covered in this thesis, analysis can continue in three ways. One, regarding the volume of attacks, future research should seek additional sources. FireEye is the only source that breaks out volume of attacks attributed to China, thus any additional data source can help prevent source bias. Additionally, as a U.S. cybersecurity firm, FireEye has a conflict of interests. Given that FireEye is contracted by the U.S. government, there is a tacit need to report a level cyberattacks to justify the company's existence and utility. Thus, reporting by third-party watchdog groups could add a better layer of credibility in judging results.

Two, as discussed in Chapter IV, many of the reports on cyberattacks lacked specific details to analyze. What data was taken? How, exactly, did the attacker gain access? The lack of such details limits the analysis. Last, better techniques and models can go a long way toward better analysis. The model used in this thesis to repurpose the Schmitt Analysis has room for improvement. Stronger definitions and parameters, particularly in cybersecurity terms, can more accurately define the results. Additionally, each cyberattack is generally composed of countless smaller attacks. From scouting to actual infiltration to exfiltration, new techniques in identifying and tying together attacks to an operation can provide better perspective on whether China is truly complying with the spirit of the Agreement or not.

With regard to future data, continuity of results is paramount for whether the Agreement is or is not a success—or, as the idiom goes, only time will tell. Two years for a bilateral agreement is still relatively short. Thus, as time passes, analysis should continue in order to better predict whether or not the trend in Chinese cyberattacks is continuing. Furthermore, as the CCP continues to make strides in cyber policy and to

form additional bilateral agreements, the United States can more accurately determine CCP intentions and progress.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. 2015 WHITE HOUSE FACT SHEET

Following is the complete White House Fact Sheet from the 2015 talks between President Xi and President Obama. The full text provides the context surrounding the 2015 U.S.-Cyber Agreement, showing the multitude of additional stipulations the two leaders discussed outside of the cyber espionage aspect discussed in this thesis.[232]

The White House
Office of the Press Secretary
For Immediate Release

September 25, 2015

FACT SHEET: President Xi Jinping's State Visit to the United States

On September 24–25, 2015, President Barack Obama hosted President Xi Jinping of China for a State visit. The two heads of state exchanged views on a range of global, regional, and bilateral subjects. President Obama and President Xi agreed to work together to constructively manage our differences and decided to expand and deepen cooperation in the following areas:

Addressing Global and Regional Challenges

- ***Afghanistan-*** The United States and China decided to maintain communication and cooperation with one another on Afghanistan to support peaceful reconstruction and economic development in Afghanistan, support an "Afghan led, Afghan owned" reconciliation process, and promote trilateral dialogue among the United States, China, and Afghanistan. Together with Afghanistan, the United States and China will co-chair a high-level event on Afghanistan's reconstruction and development on the margins of the UN General Assembly on September 26. This event will convene Afghanistan's neighbors and the international community to discuss the importance of continuing robust regional and international support for the Afghan government and regional economic cooperation. The United States and China jointly renew their call on the Taliban to enter into direct talks with the Government of Afghanistan. The United States and China also noted their mutual interests in supporting peace, stability, and prosperity in neighboring

232 "FACT SHEET: President Xi Jinping's State Visit to the United States," *The White House*, September 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

countries of Afghanistan, and to working in partnership with these countries to promote peace and stability in Afghanistan and the region.

- ***Peacekeeping-*** In recognition of the critical role UN and regional peacekeepers serve in maintaining international peace and security, the United States and China affirm to further increase their robust commitments to international peacekeeping efforts. The Chinese side appreciates the U.S. side's holding of the Leaders' Summit on Peacekeeping, and welcomes the new contributions to be announced by the United States to support peace operations. The United States welcomes the new contributions to be announced by China to support UN peacekeeping efforts. The United States and China recognize the need to deepen the partnership between the African Union and the United Nations on peace operations. Both sides look forward to an enhanced discussion with the African Union and other partners to further explore proposals to this end. Both sides decided to continue discussions to deepen cooperation on capacity building for troop- and police-contributing countries.
- ***Nuclear Security-*** The United States and China commit to deepen their cooperation on nuclear security and to work together to make the Nuclear Security Summit hosted by President Obama next year a success. The two sides plan to hold an annual bilateral dialogue on nuclear security, with the first meeting of the dialogue to be held prior to the 2016 Nuclear Security Summit.
- ***Wildlife Trafficking-*** The United States and China, recognizing the importance and urgency of combating wildlife trafficking, commit to take positive measures to address this global challenge. The United States and China commit to enact nearly complete bans on ivory import and export, including significant and timely restrictions on the import of ivory as hunting trophies, and to take significant and timely steps to halt the domestic commercial trade of ivory. The two sides decided to further cooperate in joint training, technical exchanges, information sharing, and public education on combating wildlife trafficking, and enhance international law enforcement cooperation in this field. The United States and China decided to cooperate with other nations in a comprehensive effort to combat wildlife trafficking.
- ***Ocean Conservation-*** The United States and China intend to pursue actively cooperation on polar and ocean matters, including projects related to ocean conservation and expanding joint polar research efforts, and will work together on the proposal to establish a Marine Protected Area (MPA) in Antarctica's Ross Sea. The two sides also plan to support additional bilateral efforts in these fields, including ocean acidification monitoring and a partnership between the coastal cities of Xiamen and Weihai in China

and San Francisco and New York in the United States to share best practices to reduce the flow of trash into the ocean.

Strengthening Development Cooperation

The United States and China signed a **Memorandum of Understanding** that establishes a framework for development cooperation to guide our future collaborative efforts. The MOU recognizes our shared objectives in ending extreme poverty and advancing global development through enhanced collaboration and communication under the principle of development raised, agreed, and led by recipient countries.

- ***2030 Agenda for Sustainable Development.*** The United States and China are committed to advance sustainable and inclusive international development as laid out in the new 2030 Agenda for Sustainable Development, through expanded cooperation to end poverty and hunger and the promotion of inclusive economic growth, and protection of the environment. The two sides intend to communicate and cooperate in implementing the Agenda and to help other countries achieve common development goals.
- **Food Security-** The United States and China decided to enhance cooperation on global food security. The two sides intend to enhance communication and coordination with the government of Timor Leste and share lessons learned in agricultural development and food security while exploring prospects for further cooperation. Separately, the two sides intend to explore opportunities to cooperate on climate smart agriculture to produce more and better food for growing populations, while building the resilience of smallholder farmers. Such efforts may include technical cooperation, such as on climate friendly irrigation and mechanization for smallholder farmers in Africa to advance our shared interest in addressing the impact of climate change and enhancing food security.
- **Public Health and Global Health Security-** The United States and China decided to enhance concrete cooperation in public health and global health security, accelerating full implementation of the World Health Organization International Health Regulations and assisting at-risk countries to prevent, detect, and respond to infectious disease threats. The two sides plan to jointly work with the African Union and African Union Member States in the establishment of the Africa Center for Disease Control and Prevention and collaborate with partner governments in countries in West Africa to strengthen national public health capacities in the wake of Ebola, including strengthening the capacity of the cadres of public health and front line health workers. The two sides intend to enhance communication and exchanges regarding aid for health in West Africa.

The two sides plan to continue to support and contribute to the Global Fund to Fight AIDS, Tuberculosis, and Malaria.

- **Humanitarian Assistance and Disaster Response-** The United States and China decided to expand cooperation on humanitarian response to disasters. The United States and China plan to participate constructively in the May 2016 World Humanitarian Summit. The two sides plan to expand existing cooperation on disaster response through increased support to multilateral mechanisms, including the United Nations International Search and Rescue Advisory Group. The two sides intend to conduct capacity building cooperation for the post-earthquake reconstruction in Nepal through mechanisms that promote collaboration between the international community and the Government of Nepal.
- **Multilateral Institutions.** The United States and China intend to expand their collaboration with international institutions to tackle key global development challenges.

Strengthening Bilateral Relations

- ***Military Relations-*** Building on the two Memoranda of Understanding on Confidence Building Measures (CBMs) signed by the United States and China in November 2014, the two sides completed new annexes on air-to-air safety and crisis communications. The two sides committed to continue discussions on additional annexes to the Notification of Major Military Activities CBM, with the United States prioritizing completion of a mechanism for informing the other party of ballistic missile launches. The U.S. Coast Guard and the China Coast Guard have committed to pursue an arrangement whose intended purpose is equivalent to the Rules of Behavior Confidence Building Measure annex on surface-to-surface encounters in the November 2014 Memorandum of Understanding between the United States Department of Defense and the People's Republic of China Ministry of National Defense.
- ***Cybersecurity-***
  - The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigation to the other side, as appropriate.
  - The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade

secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.

- Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International security, which addresses norms of behavior and other crucial issues for international security in cyberspace. The two sides also agree to create a senior experts group for further discussions on this topic.
- The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China will designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office will participate in the dialogue. The U.S. Secretary of Homeland Security and the U.S. Attorney General will co-chair the dialogue, with participation from representatives from the Federal Bureau of Investigation, the U.S. Intelligence Community and other agencies, for the United States. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides agree to establish a hotline for the escalation of issues that may arise in the course of responding to such requests. Finally, both sides agree that the first meeting of this dialogue will be held by the end of 2015, and will occur twice per year thereafter.

- ***Law Enforcement and Counterterrorism-*** President Obama and President Xi decided to continue expanding law enforcement and anti-corruption cooperation, including by enhancing coordination and cooperation on criminal investigations, repatriation of fugitives, and asset recovery issues. The United States and China welcomed recent progress on repatriating Chinese fugitives and illegal immigrants through charter flights and look forward to continuing this cooperation. The United States welcomes China's commitment to consider joining the OECD Working Group on Bribery as a participant in the near future. As a new aspect of the Joint Liaison Group's role as the primary mechanism for law enforcement cooperation, both sides committed to discuss the mutual recognition and enforcement of forfeiture judgments. The two sides condemn all forms of terrorism and committed to expand exchange of information to counter the transnational flow of foreign terrorist fighters. The United States and China held a Counter-Improvised Explosive Devises (IEDs) Workshop on September 14 in

Washington, DC, decided on principles for furthering efforts to counter the threat posed by IEDs, and committed to hold a follow-on workshop in China.

- ***People-to-People Exchange***. The United States and China announced two new initiatives to expand the dynamic and positive people-to-people interaction that is the foundation of our bilateral relationship: (1) A 2016 U.S.-China Tourism Year—a cooperative tourism initiative led by the U.S. Department of Commerce and the China National Tourism Administration to expand and shape travel between our countries. This year of collaboration will include events to promote travel between the two countries, support progress on market access, and advance initiatives for both the United States and China to ensure a quality visitor experience for increasing numbers of travelers to and from both nations. (2) A "One Million Strong" initiative led by the 100,000 Strong Foundation that aims to have one million American students studying Mandarin by 2020. "One Million Strong" goals include doubling the number of Mandarin language teachers in the United States through a major investment in teachers colleges; employing technological tools to engage students in underserved and underrepresented communities; and creating "100K Strong States," a subnational consortium of U.S. governors committed to expanding Mandarin language-learning in their states.

APPENDIX B. SCHMITT ANALYSIS VALUATIONS

Cyber Incident[243]	Start Date (Earliest Indication)	End Date (Last Known)	Severity	Immediacy	Directness	Invasiveness	Measurability	Presumptive Legitimacy	Responsibility	Total Value
LuckyCat	Jun-11	Apr-12	25	50	40	75	10	10	80	290
The Elderwood Project	Dec-09	Sep-12	60	60	80	75	30	25	70	400
APT 1	Feb-06	May-14	80	60	60	75	70	80	90	515
The Nitro Attacks	Apr-11	Sep-11	60	80	80	70	30	80	75	475
Night Dragon	Nov-09	Feb-11	25	30	80	65	30	80	70	380
Byzantine Hades	Apr-09	Jun-10	70	20	90	85	80	10	80	435
GhostNet	May-07	Mar-09	40	30	70	70	30	70	60	370
Honker Union	May-98	Sep-13	20	90	80	40	20	20	80	350
Wicked Rose' and the NCPH Hacking Group	May-06	Jun-07	25	70	70	40	20	20	90	335
The Chinese Time Bomb	Feb-13	Feb-13	10	10	70	40	30	80	60	300
Operation Shady RAT	Jul-06	Sep-10	20	30	60	40	20	75	20	265

Cyber Incident[243]	Start Date (Earliest Indication)	End Date (Last Known)	Severity	Immediacy	Directness	Invasiveness	Measurability	Presumptive Legitimacy	Responsibility	Total Value
Operation Aurora	Jul-09	Jan-10	20	40	60	30	20	10	50	230
Titan Rain	Nov-03	Nov-04	80	70	80	80	80	10	80	480
US Satellite Hack	Oct-07	Jul-08	70	90	90	90	90	10	30	470
State Department Emails	Apr-08	Oct-08	20						10	30
Morgan Stanley	Jan-10	Jan-10							20	20
NASA Intrusion	Jan-11	Mar-12					70		20	90
U.S. Department of Labor and at least nine other agencies	May-13	May-13							30	30
Community Health Systems	Apr-14	Jun-14	40	80	80	60	20	90	50	420
Su Bin	Jan-09	Dec-13	90	80	90	90	90	10	90	540
US TRANSCOM	Jun-12	May-13	30	30	20	50	20	10	50	210
Black Vine	Dec-12	Feb-15	30	80	80	80	30	80	70	450

Cyber Incident[243]	Start Date (Earliest Indication)	End Date (Last Known)	Severity	Immediacy	Directness	Invasiveness	Measurability	Presumptive Legitimacy	Responsibility	Total Value
SS&C Technology	Sep-16	Sep-16	60	90	90	10	90	90	15	445

243Trend Micro, "LUCKYCAT REDUX: Inside an APT Campaign with Multiple Targets in India and Japan," https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf; Gavin O'Gorman and Geoff McDonald, "The Elderwood Project," Symantec, October 2012, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf; Pierluigi Paganini, "Elderwood project, who is behind Op. Aurora and ongoing attacks?," Security Affairs, September 9, 2012, http://securityaffairs.co/wordpress/8528/hacking/elderwood-project-who-is-behind-op-aurora-and-ongoing-attacks.html; Deana Shick, "Investigating Advance Persistent Threat 1," CERT/CC Blog, Carnegie Mellon University, May 20, 2014, https://insights.sei.cmu.edu/cert/2014/05/investigating-advanced-persistent-threat-1.html; Eric Chien and Gavin O'Gorman, "The Nitro Attacks: Stealing Secrets from the Chemical Industry," accessed August 13, 2017, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf; McAfee® Foundstone Professional Services and McAfee Labs, "Global Energy Attacks: 'Night Dragon,'" McAfee, February 10, 2011, https://www.mcafee.com/hk/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf; Robert Lemos, "'Byzantine Hades' Shows China's Cyber Chops," CSO, April 21, 2011, http://www.csoonline.com/article/2128120/social-engineering/-byzantine-hades--shows-china-s-cyber-chops.html; Bill Gertz, "Stolen F-35 Secrets Now Showing Up in China's Stealth Fighter," Free Beacon, March 13, 2014, http://freebeacon.com/national-security/stolen-f-35-secrets-now-showing-up-in-chinas-stealth-fighter/;Greg Walton et al., "Tracking *GhostNet:* Investigating a Cyber Espionage Network," Information Warfare Monitor, March 29, 2009, http://www.nartv.org/mirror/ghostnet.pdf; "Honker Union Of China To Launch Network Attacks Against Japan Is A Rumor," China Hush, September 15, 2010, http://www.chinahush.com/2010/09/15/honker-union-of-china-to-launch-network-attack-against-japan-is-a-rumor/; Ken Dunham & Jim Melnick, "'Wicked Rose' and the NCPH Hacking Group," Krebs on Security, November 2011, http://krebsonsecurity.com/wp-content/uploads/2012/11/WickedRose_andNCPH.pdf; Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee, August 2011, https://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf; McAfee Labs and McAfee Foundstone Professional Services, "Protecting Your Critical Assets Lessons: Learned from 'Operation Aurora,'" McAfee, March 2010, https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf; "Operation Aurora," CognitionInt, accessed August 13, 2016, http://www.cognitionint.com/operation-aurora/; Daniel Gold, "Unit 61398: Chinese Cyber-Espionage and the Advanced Persistent Threat," InfoSec Institute, March 26, 2013, http://resources.infosecinstitute.com/unit-61398-chinese-cyber-espionage-and-the-advanced-persistent-threat/#gref; Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media Inc, 2010); Jim Wolf, "China key suspect in U.S. satellite hacks: commission," Reuters, October 28, 2011, http://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028; *United States of America v. Su Bin*, 14–1318M (2014), https://www.theglobeandmail.com/news/national/article19704622.ece/BINARY/Su+Bin+1030+complaint.pdf; Jon DiMaggio, "The Black Vine Cyberespionage Group," Symantec, August 6, 2015, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf; Jon Marino, "China Hackers Swipe Millions In Data Breach," CNBC, last updated September 19, 2016, https://www.cnbc.com/2016/09/16/china-hackers-swipe-millions-in-data-breach.html.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. ALTERNATIVE SCHMITT ANALYSIS VALUATIONS

Cyber Incident[233]	Start Date (Earliest Indication)	End Date (Last Known)	Severity	Invasiveness
LuckyCat	Jun-11	Apr-12	2	7
The Elderwood Project	Dec-09	Sep-12	2	7
APT 1	Feb-06	May-14	2	7
The Nitro Attacks	Apr-11	Sep-11	2	7
Night Dragon	Nov-09	Feb-11	2	7
Byzantine Hades	Apr-09	Jun-10	2	7
GhostNet	May-07	Mar-09	0	7
Honker Union	May-98	Sep-13	0	3
Wicked Rose' and the NCPH Hacking Group	May-06	Jun-07	1	7
The Chinese Time Bomb	Feb-13	Feb-13	0	7
Operation Shady RAT	Jul-06	Sep-10	2	7

[233] See footnote 242 for full source list.

Operation Aurora	Jul-09	Jan-10	1	7
Titan Rain	Nov-03	Nov-04	0	7
US Satellite Hack	Oct-07	Jul-08	0	7
State Department Emails	Apr-08	Oct-08	0	
Morgan Stanley	Jan-10	Jan-10	2	
NASA Intrusion	Jan-11	Mar-12	2	
U.S. Department of Labor and at least nine other agencies	May-13	May-13	0	
Community Health Systems	Apr-14	Jun-14	0	7
Su Bin	Jan-09	Dec-13	0	7
US TRANSCOM	Jun-12	May-13	0	
Black Vine	Dec-12	Feb-15	2	7
SS&C Technology	Sep-16	Sep-16	2	

APPENDIX D. 2015 U.S.-CHINA CYBER AGREEMENT DOCUMENTS

The following text provides the specific language from the three documents concerning the Agreement.

From the "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference"[234]:

> **President Obama**: I raised once again our very serious concerns about growing cyber-threats to American companies and American citizens. I indicated that it has to stop. The United States government does not engage in cyber economic espionage for commercial gain. And today, I can announce that our two countries have reached a common understanding on the way forward. We've agreed that neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage. In addition, we'll work together, and with other nations, to promote international rules of the road for appropriate conduct in cyberspace.
>
> So this is progress. But I have to insist that our work is not yet done. I believe we can expand our cooperation in this area, even as the United States will continue to use all of the tools at our disposal to protect American companies, citizens and interests.
>
> **President Xi**: China and the United States are two major cyber countries and we should strengthen dialogue and cooperation. Confrontation and friction are not made by choice for both sides. During my visit, competent authorities of both countries have reached important consensus on joint fight against cyber-crimes. Both sides agree to step up crime cases, investigation assistance and information-sharing. And both government will not be engaged in or knowingly support online theft of intellectual properties. And we will explore the formulation of appropriate state, behavior and norms of the cyberspace. And we will establish a high-level joint dialogue mechanism on the fight against cyber-crimes and related issues, and to establish hotline links.
>
> Democracy and human rights are the common pursuit of mankind. At the same time, we must recognize that countries have different historical processes and realities, and we need to respect people of all countries in the right to choose their own development path independently.

234 "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," *The White House*, September 25, 2014, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

The Chinese people are seeking to realize the great renew of the Chinese nation, which is the Chinese history. This process in essence is a process to achieve social equity and justice and advancing human rights. China stands ready to, in the spirit of equality and mutual respect, conduct human rights dialogue with the United States, expand consensus, reduce differences, learn from each other, and progress together.

President Obama: Okay, we're going to take a few questions. We're going to start with Margaret Talev of Bloomberg.

Q: Thank you, Mr. President. President Obama and President Xi, I'd like to talk to you about cyber. If I am an American business and I'm being hacked by Chinese pirates who are trying to steal my intellectual property, what firm assurances can you give us today that things are going to get better, and when?

President Obama, are you satisfied enough about the steps that China is taking to hold off on imposing any new sanctions to this end? Or what do you still need to see?

And, President Xi, could we expect prosecutions of Chinese people and organizations who have hacked American businesses? And if the U.S. did sanction anyone in China, would you respond with sanctions?

President Obama: I'll take them in order. With respect to cyber, this has been a serious discussion between myself and President Xi since we first met in Sunnylands. And the good news, from my perspective, is, is that in the lead-up to and then finalized during our meetings here today, we have, I think, made significant progress in agreeing to how our law enforcement and investigators are going to work together, how we're going to exchange information, how we are going to go after individuals or entities who are engaging in cyber-crimes or cyber-attacks. And we have jointly affirmed the principle that governments don't engage in cyber-espionage for commercial gain against companies. That all I consider to be progress.

What I've said to President Xi and what I say to the American people is the question now is, are words followed by actions. And we will be watching carefully to make an assessment as to whether progress has been made in this area.

With respect to the various tools that we have to go after those who are attacking our companies or trying to extract trade secrets or data, we have traditional law enforcement tools, but—as I indicated a while back—through executive action, I've also instituted the ability to impose sanctions on individuals or entities where we have proof that they've gone after U.S. companies or U.S. persons.

And we did not, at our level, have specific discussions of specific cases. But I did indicate to President Xi that we will apply those and whatever other tools we have in our toolkit to go after cyber criminals, either retrospectively or prospectively. Those are tools generally that are not directed at governments; they are directed at entities or individuals that we can identify. And they're not unique to China.

Those are tools that we're going to be using for cyber criminals around the world.

And President Xi, during these discussions, indicated to me that, with 1.3 billion people, he can't guarantee the behavior of every single person on Chinese soil—which I completely understand. I can't guarantee the actions of every single American. What I can guarantee, though, and what I'm hoping President Xi will show me, is that we are not sponsoring these activities, and that when it comes to our attention that non-governmental entities or individuals are engaging in this stuff, that we take it seriously and we're cooperating to enforce the law.

The last point I'll make on the cyber issue—because this is a global problem, and because, unlike some of the other areas of international cooperation, the rules in this area are not well developed, I think it's going to very important for the United States and China, working with other nations and the United Nations and other—and the private sector, to start developing an architecture to govern behavior in cyberspace that is enforceable and clear.

It doesn't mean that we're going it prevent every cyber-crime, but it does start to serve as a template whereby countries know what the rules are, they're held accountable, and we're able to jointly go after non-state actors in this area.

President Xi: (As interpreted.) Madam reporter has raised the cybersecurity issue. Indeed, at current, for the international community and for China and the United States, this is an issue all attach great importance to. With President Obama and I have on many occasions—and this is a long history—have exchange of views on this. I think it's fair to say we've reached a lot of consensus on cybersecurity, including some new consensus.

Overall, the United States is the strongest country in terms of cyber strength. China is the world's biggest cyber country in terms of the number of Web users. We have more than 600 million of netizens. Our two sides should cooperate because cooperation will benefit both, and confrontation will lead to losses on both sides. We are entirely able to carry out government department and expert levels of dialogue and exchanges to strengthen our cooperation in many respects and turn the cybersecurity between the two countries into a new growth source, rather than a point of confrontation between the two sides.

China strongly opposes and combats the theft of commercial secrets and other kinds of hacking attacks. The U.S. side, if has concerns in this respect, we can, through the exiting channels, express those concerns. The Chinese side will take seriously the U.S. provision of any information. Now, we have already, and in the future, we will still, through the law enforcement authorities, maintain communication and coordination on this matter, and appropriately address them.
So, all in all, we have broad, common interest in the field of the cyber. But we need to strengthen cooperation and avoid leading to confrontation. And nor should we politicize this issue. During my current visit, I think it's fair to say that the two sides, concerning combatting cyber-crimes, have reached a lot of consensus. Going

forward, we need to, at an early date, reach further agreement on them and further put them on the ground.

Thank you.

From the "FACT SHEET: President Xi Jinping's State Visit to the United States"[235]:

> Cybersecurity-
> The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigation to the other side, as appropriate.
> The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.
> Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International security, which addresses norms of behavior and other crucial issues for international security in cyberspace. The two sides also agree to create a senior experts group for further discussions on this topic.
> The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China will designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office will participate in the dialogue. The U.S. Secretary of Homeland Security and the U.S. Attorney General will co-chair the dialogue, with participation from representatives from the Federal Bureau of Investigation, the U.S. Intelligence Community and other agencies, for the United States. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides agree to establish a hotline for the escalation of issues that may arise in the course of responding to such requests. Finally, both sides agree that the first meeting of this dialogue will be held by the end of 2015, and will occur twice per year thereafter.

235 "FACT SHEET: President Xi Jinping's State Visit to the United States," *The White House*, September 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

From the "Full Text: Outcome list of President Xi Jinping's state visit to the United States"[236]:

> 48. China and the United States agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigation to the other side, as appropriate. China and the United States agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.
>
> Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. China and the United States welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, which addresses norms of behavior and other crucial issues for international security in cyberspace.
>
> The two sides also agree to create a senior experts group for further discussions on this topic. China and the United States agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China will designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office will participate in the dialogue. The U.S. Secretary of Homeland Security and the U.S. Attorney General will co-chair the dialogue, with participation from representatives from the Federal Bureau of Investigation, the U.S. Intelligence Community and other agencies, for the United States.
>
> This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides agree to establish a hotline for the escalation of issues that may arise in the course of responding to such requests. Finally, both sides agree that the first meeting of this dialogue will be held by the end of 2015, and will occur twice per year thereafter.

236 " Full Text: Outcome list of President Xi Jinping's state visit to the United States," The Ministry of Foreign Affairs of the People's Republic of China, September 26, 2015, http://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1300771.shtml.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Akamai. "State of the Internet/Security: Q2 2017 Report." *Akamai* 4, no. 2 (2017). https://www.akamai.com/us/en/multimedia/documents/state-of-the-Internet/q2-2017-state-of-the-Internet-security-report.pdf.

Alperovitch, Dmitri. "Revealed: Operation Shady RAT." McAfee. August 2011. https://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

———. "The Latest on Chinese-affiliated Intrusions into Commercial Companies." *Crowdstrike (*blog). October 19, 2015. https://www.crowdstrike.com/blog/the-latest-on-chinese-affiliated-intrusions-into-commercial-companies/.

———. Twitter post. December 16, 2016, 12:03 p.m. https://twitter.com/DAlperovitch/status/809851503347453954

———. "U.S.–China Agreement on Cyber Intrusions: An Inflection Point," *Crowdstrike (*blog), September 25, 2015. https://www.crowdstrike.com/blog/cyber-agreement/.

Austin, Greg. *Cyber Policy in China*. Cambridge: Polity Press, 2014.

Bender, Jeremy, and Skye Gould. "The 35 Most Powerful Militaries in the World." *Business Insider*, July 10, 2014. Accessed February 1, 2017, http://www.businessinsider.com/35-most-powerful-militaries-in-the-world-2014-.

Bengali, Shashank, Ken Dilanian, and Alexandra Zavis. "Timeline: Chinese Cyber Attack Disclosures." *Los Angeles Times,* June 5, 2013. http://timelines.latimes.com/la-fg-china-cyber-disclosures-timeline/.

Benigni, Matthew, Kathleen M. Carley, and Sumeet Kumar. "The Impact of U.S. Cyber Policies on Cyber-Attacks Trend." Carnegie Mellon University. http://www.casos.cs.cmu.edu/publications/papers/2016ImpactofUSCyber.pdf.

Blake, Andrew. "China Arrests Alleged OPM Hackers, Claims Breach Was Criminal, Not State-Sponsored." *The Washington Times*. December 3, 2015. http://www.washingtontimes.com/news/2015/dec/3/china-reportedly-arrests-alleged-opm-hackers-says-/.

Brown, Gary, and Christopher D. Yung. "Evaluating the US-China Cybersecurity Agreement, Part 3." *The Diplomat.* January 21, 2017. http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/.

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media Inc, 2010).

Chang, Amy. "Warring State: China's Cybersecurity Strategy." Center for a New American Security, December 2014. http://cfcollegefoundation.ca/wp-content/uploads/2016/08/CNAS_WarringState_Chang.pdf.

Chen, Qiheng. "Time for ASEAN to Get Serious About Cyber Crime: ASEAN Should Look to Forge Its Own Cyber Agreement." *The Diplomat*. August 2, 2017. http://thediplomat.com/2017/08/time-for-asean-to-get-serious-about-cyber-crime/.

Cheng, Ron. " Prospects for U.S.-China Cybercrime Cooperation: The Road Thus, Far." *Lawfare* (web blog), March 9, 2017. https://www.lawfareblog.com/prospects-us-china-cybercrime-cooperation-road-thus-far.

Chien, Eric, and Gavin O'Gorman. "The Nitro Attacks: Stealing Secrets from the Chemical Industry." Symantec. Accessed August 13, 2017. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf.

Chin, Josh. "Inside the Slow Workings of the U.S.-China Cybersecurity Agreement." The *Wall Street Journal* (blog). June 15, 2016. https://blogs.wsj.com/chinarealtime/2016/06/15/inside-the-slow-workings-of-the-u-s-china-cybersecurity-agreement/.

China Daily. "Full text: China's Military Strategy." Last updated May 26, 2015. Accessed August 25, 2017. http://www.chinadaily.com.cn/china/2015-05/26/content_20820628_4.htm.

China Hush. "Honker Union Of China To Launch Network Attacks Against Japan Is A Rumor." September 15, 2010. http://www.chinahush.com/2010/09/15/honker-union-of-china-to-launch-network-attack-against-japan-is-a-rumor/.

China.org.cn. "China's Foreign Policies for Pursuing Peaceful Development." Accessed August 25, 2017. http://www.china.org.cn/government/whitepaper/2011-09/06/content_23362744.htm.

CognitionInt. "Operation Aurora." Accessed August 13, 2016. http://www.cognitionint.com/operation-aurora/.

Creemers, Roger. "National Cyberspace Security Strategy." *China Copyright and Media* (blog). December 27, 2016. Accessed September 4, 2017. https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

CSIS. “Bilateral Discussions on Cooperation in Cybersecurity China Institute of Contemporary International Relations (CICIR) - Center for Strategic and International Studies (CSIS).” June 2012. Accessed August 26, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/120615_JointStatement_CICIR.pdf.

———. “Significant Cyber Incidents Since 2006.” Center for Strategic and International Studies, Accessed August 1, 2017. https://www.csis.org/programs/technology-policy-program/cybersecurity/other-projects-cybersecurity/significant-cyber.

deLisle, Jacques, and Jeffrey Vagle. “The Download on the U.S.-China Cyber Espionage Agreement.” Wharton. September 30, 2015. http://knowledge.wharton.upenn.edu/article/the-download-on-the-u-s-china-cyber-espionage-agreement/.

Department of Homeland Security. “First U.S.-China High Level Joint Dialogue on Cybercrime and Related Issues.” December 2, 2015. https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0.

———. “Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue.” June 14, 2016. https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue.

———. “Third U.S.-China High Level Joint Dialogue on Cybercrime and Related Issues.” December 8, 2016. https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues.

Dilanian, Ken. “Russia May Be Hacking Us More, But China Is Hacking Us Much Less.” NBC News. October 12, 2016. http://www.nbcnews.com/storyline/hacking-in-america/russia-may-be-hacking-us-more-china-hacking-us-much-n664836.

DiMaggio, Jon. “The Black Vine Cyberespionage Group.” Symantec. August 6, 2015. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf.

Dunham, Ken, and Jim Melnick. “‘Wicked Rose’ and the NCPH Hacking Group.” Krebs on Security. November 2012. http://krebsonsecurity.com/wp-content/uploads/2012/11/WickedRose_andNCPH.pdf.

Eder, Thomas, Bertram Lang, and Moritz Rudolf, “China’s Global Law Enforcement Drive: The Need For A European Response.” Mercator Institute for China Studies. January 18, 2017. https://www.merics.org/en/merics-analysis/china-monitor/merics-china-monitor-no-36/#c17722.

Ellis, Jamie. "Chinese Cyber Espionage: A Complementary Method to Aid PLA Modernization," Master's thesis, Naval Postgraduate School, 2015. https://calhoun.nps.edu/bitstream/handle/10945/47941/15Dec_Ellis_Jamie.pdf?sequence=1&isAllowed=y.

Eng, Eric, and Dan Caselden. "Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign." FireEye. June 23, 2015. https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html.

Europol. "The Geographical Distribution Of Cybercrime." Accessed August 21, 2017. https://www.europol.europa.eu/iocta/2015/distribution.html.

FireEye. "Advanced Persistent Threat Groups." Accessed May 15, 2017. https://www.fireeye.com/current-threats/apt-groups.html#apt30.

———. "APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat." April 6, 2017. https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html.

———. "Redline Drawn: China Recalculates its use of Cyber Espionage." June 2016. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

Foltz, Andrew C. "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate." *JFQ* 67 (2012).

Gandel, Stephen. "Lloyd's CEO: Cyber attacks cost companies $400 billion every year." Fortune. January 23, 2015. Accessed March 02, 2017. http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/.

Gechlik, Mel. "Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for U.S. Businesses." Hoover Institution. *Aegis Series Paper,* no. 1706. http://www.hoover.org/sites/default/files/research/docs/gechlik_webreadypdf.pdf.

Gertz, Bill. "Stolen F-35 Secrets Now Showing Up in China's Stealth Fighter." Free Beacon. March 13, 2014. http://freebeacon.com/national-security/stolen-f-35-secrets-now-showing-up-in-chinas-stealth-fighter/.

Gibbs, Samuel. "Criminal Gang Arrested For Selling Apple Users' Private Data In China." The Guardian,. June 9, 2017. https://www.theguardian.com/technology/2017/jun/09/apple-employees-arrested-selling-private-user-data-china-criminal

Glenn, H. Patrick. *Legal Traditions of the World: Sustainable Diversity in Law*. Fifth edition. Oxford, United Kingdom: Oxford University Press, 2014.

Gold, Daniel. "Unit 61398: Chinese Cyber-Espionage and the Advanced Persistent Threat." InfoSec Institute. March 26, 2013. http://resources.infosecinstitute.com/unit-61398-chinese-cyber-espionage-and-the-advanced-persistent-threat/#gref.

Google Ideas, and Arbor Network. "Digital Attack Map." Accessed May 15, 2017. http://www.digitalattackmap.com/.

Gould, Jeremy Bender, and Skye. "The 35 Most Powerful Militaries in the World." Business Insider. July 10, 2014. Accessed February 1, 2017. http://www.businessinsider.com/35-most-powerful-militaries-in-the-world-2014-7.

Hannas, William C., James Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernization.* New York: Routledge, 2013.

Harold, Scott Warren. "The US-China Cyber Agreement: A Good First Step." *The Cipher Brief,* July 31, 2016. https://www.thecipherbrief.com/article/tech/us-china-cyber-agreement-possibly-good-first-step-1092.

Harold, Scott Warren, Martin C. Libicki, and Astrid Cevallos. *Getting to Yes with China in Cyberspace.* Santa Monica, CA: RAND Corporation, 2016. http://www.rand.org/pubs/research_reports/RR1335.html.

Hathaway, Melissa E. *Strategic Advantage: Why America Should Care About Cybersecurity.* Report. October 2009. Accessed February 15, 2017. http://www.belfercenter.org/sites/default/files/legacy/files/Hathaway.Strategic%20Advantage.Why%20America%20Should%20Care%20About%20Cybersecurity.pdf .

Heinl, Caitríona H. "New Trends in Chinese Foreign Policy: The Evolving Role of Cyber." *Asian Security* 13, no. 2 (March 2017): 132–147. Doi: 10.1080/14799855.2017.1286160.

Hennessey, Susan, and Chris Mirasola. "Did China Quietly Authorize Law Enforcement to Access Data Anywhere in the World?" Lawfare. March 27, 2017.

Ikenson, Daniel. "Cybersecurity or Protectionism?: Defusing the Most Volatile Issue in the U.S.-China Relationship" *CATO Institute* no. 815 (July 13, 2017).

Information Office of the State Council. “China’s Peaceful Development.” The State Council of the People’s Republic of China. Accessed August 8, 2017. http://www.gov.cn/english/official/2011-09/06/content_1941354.htm

Information Office of the State Council. “The Internet in China - China.org.cn.” China.org.cn. June 8, 2010. Accessed August 8, 2017. http://www.china.org.cn/government/whitepaper/node_7093508.htm

InfoSecurity. “The U.S. vs. China: A Very Civil (Cyber) War.” June 26, 2012, https://www.infosecurity-magazine.com/magazine-features/the-us-vs-china-a-very-civil-cyber-war/.

Inkster, Nigel. *China’s Cyber Power*. Abingdon: Routledge, 2016.

Keely, David M. “CYBER ATTACK! CRIME OR ACT OF WAR” (Strategy Research Project, U.S. Army War College, 2011).

Krebs, Brian. “Equifax Breach Response Turns Dumpster Fire.” Krebs on Security. September 17, 2017. Accessed November 17, 2017. https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/.

Lawrence, Susan V. China’s Political Institutions and Leaders in Charts (CRS Report No. R43303) (Washington, DC: Congressional Research Service, 2015). https://fas.org/sgp/crs/row/R43303.pdf.

———. U.S.-China Relations: An Overview of Policy Issues (CRS Report No. R41108) (Washington, DC: Congressional Research Service, 2013). https://fas.org/sgp/crs/row/R41108.pdf.

Leal, Donald. “Saving Fisheries with Free Markets,” *The Milken Institute Review* 57, no. 1(2006): 56–66.

Lemos, Robert. “‘Byzantine Hades’ Shows China’s Cyber Chops.” CSO. April 21, 2011. http://www.csoonline.com/article/2128120/social-engineering/-byzantine-hades--shows-china-s-cyber-chops.html.

Lewis, James A. “China’s Information Controls, Global Media Influence, and Cyber Warfare Strategy.” Center for Strategic and International Studies. May 4, 2017. https://www.uscc.gov/sites/default/files/James%20Lewis%20May%204th%202017%20USCC%20testimony.pdf.

———. “Sustaining Progress in International Negotiations on Cybersecurity.” Center for Strategic and International Studies. July 2017.

Li, Jiang. “Commentary: China, biggest victim of cybercrime, champions ‘community of common destiny’ in cyberspace.” Xinhua. December 16, 2015. Accessed September 13, 2017. http://news.xinhuanet.com/english/2015-12/16/c_134923452.htm.

Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” *International Security* 39, no. 3 (Winter 2014/15): 7–47. https://doi.org/10.1162/ISEC_a_00189.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron. *China and Cybersecurity: Espionage, Strategy, and Politics In The Digital Domain*. New York: Oxford University Press, 2015.

“List of Countries by Projected GDP.” StatisticsTimes. Accessed February 1, 2017. http://statisticstimes.com/economy/countries-by-projected-gdp.phpMandiant. “APT1: Exposing One of China’s Cyber Espionage Units.” (Special report, Mandiant, February 2013). https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Marino, Jon. “China Hackers Swipe Millions In Data Breach.” CNBC. Last updated September 19, 2016. https://www.cnbc.com/2016/09/16/china-hackers-swipe-millions-in-data-breach.html.

Marks, Joseph. “Obama, Xi vow not to steal each others’ secrets.” *Politico*, September 25, 2015. Accessed March 11, 2017. http://www.politico.com/story/2015/09/obama-xi-vow-not-to-steal-each-others-secrets-214077.

McAfee. *Net Losses: Estimating the Global Cost of Cybercrime*. Report. June 2014. Accessed February 15, 2017. https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

———. “2016 Threats Predictions” (report, McAfee, 2016). https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

McAfee® Foundstone Professional Services and McAfee Labs. “Global Energy Attacks: ‘Night Dragon.’” McAfee. February 10, 2011. https://www.mcafee.com/hk/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

McAfee Labs, and McAfee Foundstone Professional Services. “Protecting Your Critical Assets Lessons: Learned from ‘Operation Aurora.’” McAfee. March 2010. https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.0

Michael, James B., Thomas C. Wingfield, and Duminda Wijesekera. "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System." In *Proc. of 27th Annual International Computer Software and Applications Conference*, 622–626. November 3–6, 2003.

Milian, Mark, and Jordan Robertson. "China-Based Cyber Attacks Rise at Meteoric Pace." Bloomberg. April 23, 2013. Accessed August 21, 2017. https://www.bloomberg.com/news/2013-04-23/china-based-cyber-attacks-rise-at-meteoric-pace.html.

Ministry of Foreign Affairs of the People's Republic of China. "China Reacts Strongly to U.S. Announcement of Indictment Against Chinese Personnel." May 20, 2014. Accessed March 3, 2017. http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/t1157520.shtml.

———. "Full Text: Outcome list of President Xi Jinping's state visit to the United States." September 26, 2015. http://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1300771.shtml.

Mirasola, Chris. "Understanding China's Cybersecurity Law," Lawfare. November 8, 2016. Accessed September 4, 2017. https://www.lawfareblog.com/understanding-chinas-cybersecurity-law.

Moran, Ned, Mike Scott, Mike Oppenheim, and Joshua Homan. "Operation Double Tap." FireEye. November 21, 2014. https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html"

Morgan, Steve. *Hackerpocalypse: A Cybercrime Revelation.* Report, 2016. Accessed February 15, 2017. https://www.herjavecgroup.com/wp-content/uploads/2016/08/Hackerpocalypse.pdf.

Mozur, Paul. "New Rules in China Upset Western Tech Companies." *The New York Times.* January 28, 2015.

Mussington, David A. "The Missing Compliance Framework in the 2015 U.S.-China Cybersecurity Agreement." Institute for Defense Analysis. November 18, 2015. https://www.ida.org/~/media/Corporate/Files/Publications/IDA_Documents/ITSD/2015/D-5648.ashx;

Nakashima, Ellen. "China Still Trying to Hack U.S. Firms Despite Xi's Vow to Refrain, Analysts Say." *The Washington Post*. October 19, 2015. https://www.washingtonpost.com/world/national-security/china-still-trying-to-hack-us-firms-despite-xis-vow-to-refrain-analysts-say/2015/10/18/d9a923fe-75a8-11e5-b9c1-f03c48c96ac2_story.html?utm_term=.4189a87c6d10.

Nakashima, Ellen, and Adam Goldman. “In a first, Chinese hackers are arrested at the behest of the U.S. government.” *The Washington Post*. October 9, 2015. https://www.washingtonpost.com/world/national-security/in-a-first-chinese-hackers-are-arrested-at-the-behest-of-the-us-government/2015/10/09/0a7b0e46-6778-11e5-8325-a42b5a459b1e_story.html?postshare=9811444395972124&utm_term=.ec6e708bb6cd.

NetMarketShare. “Desktop Browser Version Market Share.” Accessed May 15, 2017. https://www.netmarketshare.com/browser-market-share.aspx?qprid=2&qpcustomd=0.

Ng, Yi Shu. “China Arrests Hackers Behind One Of The World’s Largest Malware Infections.” Mashable. July 26, 2017. http://mashable.com/2017/07/26/chinese-hackers-arrested/#_8_MAq3ZSgqn.

Norse. “Global Perspective.” December 12, 2015. Accessed August 21, 2017. http://www.norsecorp.com/wp-content/uploads/2015/12/December-2015-global-stats.pdf.

Nye, Jr., Joseph S. “The Challenge of China.” In *How to Make America Safe: New Policies for National Security.* Edited by Stephen Van Evera, 73–77. Cambridge, MA: The Tobin Project, 2006. https://tobinproject.org/sites/tobinproject.org/files/assets/Make_America_Safe_The_Challenge_Of_China.pdf, 74.

O’Brien, Robert, and Shiran Shen. “Cybersecurity between the United States and China.” Policy Innovations. May 28, 2013. Accessed March 11, 2017. http://www.policyinnovations.org/ideas/commentary/data/000260.

O’Gorman, Gavin, and Geoff McDonald. “The Elderwood Project.” Symantec. October 2012, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf.

O’Hanlon, Michael E., and James B. Steinberg. “The Trump-Xi summit: A Rocky Relationship Takes Center Stage.” Brookings. April 07, 2017. Accessed May 15, 2017. https://www.brookings.edu/blog/order-from-chaos/2017/04/07/the-trump-xi-summit-a-rocky-relationship-takes-center-stage/.

Olenick, Doug. “U.S.-China Cyber Agreement: Flawed, but a step in the right direction.” SC Media. January 24, 2017. Accessed March 11, 2017. https://www.scmagazine.com/us-china-cyber-agreement-flawed-but-a-step-in-the-right-direction/article/633533/.

Paganini, Pierluigi. “Elderwood project, who is behind Op. Aurora and ongoing attacks?” Security Affairs. September 9, 2012. http://securityaffairs.co/wordpress/8528/hacking/elderwood-project-who-is-behind-op-aurora-and-ongoing-attacks.html.

Passeri, Paolo. “2016 Cyber Attack Statistics.” January 19, 2017. Accessed April 28, 2017. http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/

People’s Daily Online. “Constitution of the People’s Republic of China.” Accessed August 24, 2017. http://en.people.cn/constitution/constitution.html.

Qu, Weizhi. *Chinas Path to Informatization*. Singapore: Cengage Learning Asia, 2010.

Red24. “Cybercrime Top 10 Countries Where Attacks Originate.” British Bankers’ Association. Accessed August 21, 2017. https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+countries+where+attacks+originate+-++2015.pdf.

Reuters. “The Us Government Might Be The Biggest Hacker In The World.” Last edited May 12, 2013. Accessed August 21, 2017. https://www.rt.com/usa/us-hacking-exploits-millions-104/.

———. “Hackers R U: China Ranks Us As Top Source Of Cyber Attacks This Year.” Last edited March 10, 2013. Accessed August 21, 2017. https://www.rt.com/news/china-blames-us-hacking-051/.

Richter, Felix. “The Web Is Turning Its Back on Flash.” December 12, 2016. Accessed May 15, 2017. https://www.statista.com/chart/3796/websites-using-flash/

Rifai, Ryan. “China Says Thousands Arrested For Online Crime.” Al Jazeera. August 18, 2018. http://www.aljazeera.com/news/2015/08/china-thousands-arrested-online-crime-150818192622887.html.

Rinehart, Ian E. “The Chinese Military: Overview and Issues for Congress” (CRS Report No. R44196). Washington, DC: Congressional Research Service, 2016. https://fas.org/sgp/crs/row/R44196.pdf.

Rogers, Vaughn C. “The History of Chinese Cybersecurity: Current Effects on Chinese Society Economy, and Foreign Relations” Master’s thesis, Seton Hall University, 2016. http://scholarship.shu.edu/dissertations/2207.

Rogin, Josh. “NSA Chief: Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History.’” Foreign Policy. July 9, 2012. http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

Rollins, John W. *U.S.-China Cyber Agreement* (CRS Report No. IN10376). Washington, DC: Congressional Research Service, 2015. https://fas.org/sgp/crs/row/IN10376.pdf.

Sacks, Samm. "China's Cybersecurity Law Takes Effect: What to Expect." Lawfare. June 1, 2017. Accessed September 1, 2017. https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

Saporito, Laura, and James A. Lewis. *Cyber Incidents Attributed to China.* Report. CSIS, March 11, 2013. Accessed February 15, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130314_Chinese_hacking.pdf

Schmitt, Michael N. "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy,* 151–177. Washington, DC: National Academies Press, 2010.

———. "Computer Network Attack And The Use Of Force In International Law: Thoughts On A Normative Framework." *Columbia Journal of Transnational Law* 37 (1999): 887–937.

Segal, Adam. "China and the United States Have an Eerily Similar Approach to Data Sovereignty." Council on Foreign Relations Blog. March 29, 2017.

Segal, Adam. "Chinese Cyber Diplomacy in a New Era of Uncertainty." Hoover Institution, *Aegis Series Paper*, no. 1703. http://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.

Segal, Adam. "The Continued Importance of the U.S.-China Cyber Dialogue." Council on Foreign Relations Blog. March 29, 2017.

———. "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?" *Council on Foreign Relations* (blog). June 29, 2017. https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

———. "The U.S.-China Cyber Espionage Deal One Year Later." *Council on Foreign Relations* (blog). September 28, 2016. https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

Setser, Brad W. "Have the Economic Constraints on China's Geostrategic Ambitions Dimished?" Council on Foreign Relations. July 17, 2017.

Shick, Deana. “Investigating Advance Persistent Threat 1.” CERT/CC Blog. Carnegie Mellon University. May 20, 2014. https://insights.sei.cmu.edu/cert/2014/05/investigating-advanced-persistent-threat-1.html.

Spidalieri, Francesca. *Understanding Cyber Threats: Lessons for the Boardroom,* report, September 2016. Accessed February 15, 2017. http://pellcenter.org/wp-content/uploads/2016/09/Understanding-Cyber-Threats-Lessons-for-the-Boardroom.pdf.

Standing Committee of the National People’s Congress. “2016 Cybersecurity Law.” China Law Translate. November 7, 2016. Accessed September 4, 2017. http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en.

Sulmeyer, Michael, and Amy Chang, “Three Observations on China’s Approach to State Action in Cyberspace,” *Lawfare* (blog). January 22, 2017. https://www.lawfareblog.com/three-observations-chinas-approach-state-action-cyberspace.

Symantec. “Buckeye Cyberespionage Group Shifts Gaze from U.S. to Hong Kong.” September 6, 2016. https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong.

Symantec. “Internet Security Threat Report” (report, Symantec, April 2017). http://s1.q4cdn.com/585930769/files/doc_downloads/lifelock/ISTR22_Main-FINAL-APR24.pdf.

Tait, Matt. Twitter post, 21 June 2016, 11:43 a.m. https://twitter.com/pwnallthethings/status/745280882076958720.

———. Twitter post, 7 September 2017, 10:19 p.m. https://twitter.com/pwnallthethings/status/906024217371525120.;

Tehran, Rita. Cybersecurity: Data, Statistics, and Glossaries (CRS Report No. R43310) (Washington, DC: Congressional Research Service, 2015). https://fas.org/sgp/crs/misc/R43310.pdf.

Tiezzi, Shannon. “China’s Response to the U.S. Cyber Espionage Charges.” *The Diplomat,* May 21, 2014. Accessed March 3, 2017. http://thediplomat.com/2014/05/chinas-response-to-the-us-cyber-espionage-charges/.

———. “The Limits of a US-China Cyber Deal.” The Diplomat. September 22, 2015. https://thediplomat.com/2015/09/the-limits-of-a-us-china-cyber-deal/.

Trend Micro. "LUCKYCAT REDUX: Inside an APT Campaign with Multiple Targets in India and Japan." https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf.

United States of America vs Wang Dong, Sun Kailing, Wen Xinyu, Huang Zhenyu, Gu Chunhui. No. 14–118 (PA, District Ct, Western District May 1, 2014). https://www.justice.gov/iso/opa/resources/512201451913235846 1949.pdf.

United States of America v. Su Bin. 14–1318M (2014). https://www.theglobeandmail.com/news/national/article19704622.ece/BINARY/Su+Bin+1030+complaint.pdf.

U.S.-China Economic and Security Review Commission "2015 Annual Report to Congress." November 2015. http://origin.www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF.

———. "China's Intelligence Services And Espionage Operations." June 9, 2016. https://www.uscc.gov/sites/default/files/transcripts/June%2009%2C%202016%20Hearing%20Transcript.pdf.

———. "Hearing Before the U.S.-China Economic and Security Review Commission." June 09, 2016. https://www.uscc.gov/sites/default/files/transcripts/June%2009,%202016%20Hearing%20Transcript.pdf.

U.S. Department of Defense, "US Nuclear Posture Review Report April 2010: Executive Summary." U.S. Department of Defense, April 2010, https://www.defense.gov/Portals/1/features/defenseReviews/NPR/2010_Nuclear_Posture_Review_Report.pdf.

U.S. Department of Justice. "First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes." December 2, 2015. https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0.

———. "Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue." June 14, 2016. https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue.

———. "Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues." December 8, 2016. https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues.

Umhoefer, Carol A. F., Carolyn Bigg, Stefan Panic, Tomomi Fujikouge, and Louise Crawford. “China: First 100 Days Of Cybersecurity Law Sees Active Enforcement, More Guidelines But Still Uncertainties.” *Lexology* (blog). September 4, 2017. https://www.lexology.com/library/detail.aspx?g=fcbcf874-456f-412a-b30c-9b78fe4a3e6b.

Verizon. “2016 Data Breach Investigations Report” (report, Verizon, 2016)

———. “2017 Data Breach Investigations Report” (report, Verizon, 2017).

W3Counter. “Browser & Platform Market Share.” Accessed May 15, 2017. https://www.w3counter.com/globalstats.php.

W3Techs. “Usage of Flash for websites.” Accessed May 15, 2017. https://w3techs.com/technologies/details/cp-flash/all/all.

Walton, Greg, Ronald Deibert, Arnav Manchanda, Rafal Rohozinski, Nart Villeneuve, Jane Gowan, Belinda Bruce, and James Tay. “Tracking *GhostNet:* Investigating a Cyber Espionage Network.” Information Warfare Monitor. March 29, 2009. http://www.nartv.org/mirror/ghostnet.pdf.

Waters, Riley. “Cyber Attacks on U.S. Companies in 2014.” Oct 27, 2014. http://thf_media.s3.amazonaws.com/2014/pdf/IB4289.pdf.

———. “Cyber Attacks on U.S. Companies Since November 2014.” November 18, 2015. http://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014.

———. “Cyber Attacks on U.S. Companies in 2016.” The Heritage Foundation, December 2, 2016. http://www.heritage.org/defense/report/cyber-attacks-us-companies-2016.

Weibin, Zhao. “The Four Stages of Sino-American Cyber Relations.” China U.S. Focus. October 9, 2017. https://www.chinausfocus.com/peace-security/the-four-stages-of-sino-american-cyber-relations.

The White House. “Executive Order – ‘Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.’” April 1, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

———. “FACT SHEET: President Xi Jinping’s State Visit to the United States.” September 25, 2015. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

———. “Remarks by President Obama and President Xi of the People’s Republic of China in Joint Press Conference.” September 25, 2014. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

Wolf, Jim. “China Key Suspect in U.S. Satellite Hacks: Commission.” Reuters. October 28, 2011. http://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028.

Xinhua. “China, U.S. discuss int’l norms of state behavior in cyberspace.” May 12, 2016. http://news.xinhuanet.com/english/2016-05/12/c_135354264.htm.

———. “Full Text: International Strategy of Cooperation on Cyberspace.” March 1, 2017. Accessed September 4, 2017. http://news.xinhuanet.com/english/china/2017-03/01/c_136094371_4.htm.

Zetter, Kim. “US and China Reach Historic Agreement on Economic Espionage.” Wired. September 25, 2015. https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/.

HIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California