Getting Harder to Catch

Analyzing the Evolution of China's Cyber Espionage Campaigns against the United States through a Case Study of APT1

Winnona DeSombre – Comp116 Security Final Paper

Advisor: Ming Chow

1. Abstract

The relationship between China and the United States is arguably one of the more thorny dynamics in the sphere of international politics, complicated further by each country's increasing cyber espionage and cyber warfare capabilities. As early as 2007, the US-China Economic and Security Review Commission has labeled China's espionage efforts "the single greatest risk to the security of American technologies"[1]. However, as cyber security is a relatively new field in international relations, there is little set precedence for pressing charges or taking other action against individuals or groups conducting cyber attacks or espionage. This paper is composed of three parts: part one contains an overview of China-US relations within the context of the cyber realm and dilemmas in the international sphere regarding formulation of cyber security policy. Part two is a case study of the hacker unit APT1, a hacker unit argued to be the Chinese People's Liberation Army Unit 61398, which covers both APT1's history and an analysis of its cyber espionage campaigns. Part three reviews the general trends of APT1 within the context of the 2015 US-China Cyber Agreement and China-US relations regarding cyber security in general, and how the trends can possibly impact future actions of international actors and state-sponsored hacker groups.

2. To the Community: Defining Critical Infrastructure & Setting Policy Boundaries

Policy often moves at a slower pace than technical innovation, especially when compared to the exponential rates of technological change in cyber capabilities. Four factors add to the difficulty of formulating cyber policy: the lack of shared terminology (both between states and within technical industries), the lack of "net natives" among senior policymakers, difficulty of attributing a cyber attack to a specific actor with complete confidence (also known as "the attribution problem"), and the

1 . Claburn, "China Cyber Espionage"

fundamental offense/defense paradigm within the cyber sphere that favors the attacker [2]. These factors, when grinding the creation of policy regarding cyber exploits or attacks that damage or incapacitate critical networks to a standstill, make the situation even worse in the sphere of cyber espionage policy. Most international scholars agree that, although many international cyber campaigns are often described as “attacks”, a majority of these campaigns exclusively use cyber espionage – the use of computer networks to gain unlawful access to confidential information – which does not an act of war. On the contrary, similarly to regular espionage, cyber espionage is assumed to happen between most countries[3]. However, when a hack is discovered and blame is placed on a state actor, there are few norms or international laws that dictate how a country’s government should respond. This is partially because of the difficulty of attributing a hack to specific individuals within the state, rather than the state itself. Thus, many state actors will aggressively use media outlets to broadcast their anger at being hacked, but will do little else. The same can be said between China and the United States, two countries that are extraordinarily dependent on each other economically.

3. Introduction

i. Trends in Cyber Espionage in China-US Relations

Starting in the early 2000’s, databases of key United States companies and government agencies were frequently being broken into by outside actors keen on accessing confidential data – in both the public and private sectors – for both economic and political gain. One of the largest industrial cyber espionage campaigns at the time, Operation Aurora, was attributed to hackers within the Chinese government. The campaign, which went unnoticed for six months, targeted approximately 34 companies, many of which were in the information technology industry. While experts agree that the

2 . Lieberthal, Singer. "Cybersecurity and U.S.-China Relations", vii
3 . Lewis, *“A Note on the Laws of War in Cyberspace”, 1*

campaign was largely for economic gain, hackers also accessed information important to US national security: confidential information, including US wiretapped Gmail accounts, was compromised in the attacks[4]. In response to accusations of espionage, China issued a statement that it opposed all hacking, and was itself a victim of cyber attacks orchestrated by the US[5]. This was not an unfair statement – The Chinese Ministry of Public Security has noted that the "number of cyber attacks on Chinese computers and websites has soared by more than 80 percent annually, and, by the raw numbers, China is the world's largest victim of cyber attacks". Moreover, it is undeniable that a large amount of malicious Internet activity emanates from or at least moves through the United States[6]. While Google moved quickly to stop censoring its Chinese service[7], very little was done by the US government in response to the alleged state-sponsored hack. Thus began a pattern of breaches, US policymakers erring on the side of caution in accusing China, and blanket denials of culpability by the Chinese government amidst the increased levels of private-sector allegations.

ii. The Rise of APTs

Operation Aurora also marked the rise of advanced persistent threats (APTs): a group of individuals (state-sponsored or otherwise), using stealthy and continuous computer hacking processes to pick on a specific target or set of targets. An APT would usually use sophisticated malware to exploit vulnerabilities in target systems and set up an external command and control system that continuously monitored and extracted data from the target, stealing terabytes of data over an extended period of time[8]. An attack conducted by an APT can be described in five phases: reconnaissance (doing research on a company to determine what desired information can be stolen and crafting possible plans for

4 Naked Security, "Project Aurora"
5 Branigan, "China Responds to Google Hacking Claims"
6 . Lieberthal, Singer. "Cybersecurity and U.S.-China Relations", 6
7 Branigan, "China Responds to Google Hacking Claims"
8 Sullivan, "Beyond the Hype, Advanced Persistent Threats", 4

intrusion), incursion (gaining access to the target computers or network), discovery (seeing what information is actually accessible and desirable, and the location of said information), capture (obtaining desired information by gaining the privileges to do so) and exfiltration (sending the information back to the APT's local network)[9]. While arguably the most famous APT, STUXNET, originated from the United States[10], China is considered by many to be one of the most active and capable APT users[11]. One advanced persistent threat in particular, APT1, has been attributed to a secret unit within China's military – the People's Liberation Army (PLA). Although the concept of APTs had been introduced over a decade ago, China's APT1 launched advanced persistent threats (state-sponsored or otherwise) into the public eye.

4. APT1: Tactics and Tools

APT1 was a particular Chinese hacker group whose first compromise occurred around 2006. Since then, they have stolen large volumes of intellectual property (blueprints, test results, proprietary manufacturing processes etc) from at least 141 organizations across both commercial and national security industries[12]. What makes APT1 particularly interesting are the following: APT1 almost solely targets English-speaking organizations, more than 80% of which are located in the United States. Their incursion method of choice is spear phishing – writing targeted emails to specific members of a company containing malicious attachments that, when opened, infect the target's computer[13]. Although APT1, the name given to the group by cyber security group Mandiant, is the name most commonly used to refer to the group since 2013, its other names include "the Comment Group" or "the Comment Crew". These names stem from the hacker group's habit to conduct their command-and-control

9 Scheier, Bruce. "The Story Behind the Stuxnet Virus"
10 The STUXNET virus, which nearly took down the Irani nuclear program, was discovered only six months after Operation Aurora and attributed to the US and Israeli governments.
11 InfoSec, "Current Trends in the APT World"
12 Mandiant. "APT1: Exposing one of China's Cyber Espionage Units", 3
13 Ibid, 5.

communications through HTML comments – sentences written in code normally for a programmer's benefit that do not show up on the rendered HTML page itself[14].

i. APT1's Attack Cycle

APT1's attack cycle contains all the five phases of an average APT attack, but instead of deleting any trace of compromise post-mission, APT1 will continue to steal information from a target, in most cases, as long as they still have access to the network[15].

Reconnaissance and Incursion

Spear-phishing has played an imperative role in the success of APT1's cyber espionage campaigns. Spear-phishing is the attempt to obtain sensitive information or send malware via email (aka phishing), but using information gleaned through research to target the specific email recipient (eg. a coworker's name or a document regularly produced by one's place of work). In the case of APT1, the emails would appear to be sent by a target's superior, asking them to download an attachment in the form of a .zip file. If the target replied to the email, APT1 would even reply in English, still encouraging them to open the attachment[16]. When the target decompressed the zip file and opened all the files inside, malware (usually in an executable .exe file) would run and install itself onto the host computer. On some occasions, the malware would be further disguised to not look like a .exe file. To further hide their tracks and encourage the target to click on all the files, APT1 actors would rename an executable file to have common job-related fake file extensions, such as zip, jpeg, doc, etc For example, a piece of malware "backdoor.exe" would be changed to "ImportantBriefing.pdf.exe"),

14 Sophos. "Mandiant APT1 (Comment Crew) Response"
15 Mandiant. "APT1: Exposing one of China's Cyber Espionage Units", 29
16 Ibid, 30.

with 100 spaces after the filename and the .exe extension, such that the file would show up in the user's file viewer as "ImportantBriefing.pdf..."[17].

When the malware was run, the program would make an HTTP connection to a Command and Control (C2) server: a centralized computer that could issue commands to the program and receive reports back from the program itself. This became APT1's backdoor into the system – the HTTP connection allowed the APT1 attacker to send commands to the system and bypass all firewalls, as the target computer itself had initialized the connection[18]. The attacker then could download all sorts of other backdoor software[19] into the system. APT1 mainly used two kinds of back-doors: WEBC2 backdoors (or Beachhead backdoors) and non-WEBC2 backdoors – although most were customized and written by APT1 itself. A WEBC2 backdoor makes an HTTP request to the C2 Server, requesting an HTML page, and will interpret the webpage's special HTML tags (or comments), as commands. As APT1 would frequently put their malicious commands within HTML comments, much of the international computer security community also refer to APT1 as "the Comment Crew". WEBC2 backdoors allowed APT1 attackers to execute rudimentary command shell instructions, download and execute a file, and instruct their malware to be inactive for a set period of time. [20] The non-WEBC2 backdoors used by APT1 also communicated through HTTP or through a custom protocol designed by APT1 itself. These backdoors were more complicated and effectively gave the attacker full control of the target computer, and access to the network that the computer was on. Additionally, many of APT1's backdoors used SSL encryption such that communications between the C2 server and the targeted computer were hidden.

17 Yip, Ki Nang. "Spear-Phishing Case Study."
18 Mandiant. "APT1: Exposing one of China's Cyber Espionage Units", 31
19 Backdoor software: software that allows an intruder access to a computer that bypasses security mechanisms.
20 Mandiant. "APT1: Exposing one of China's Cyber Espionage Units", 32

[21]

```
GET /css/about.htm HTTP/1.1
User-Agent: Microsoft Internet Explorer Exelon MYHOSTNAME
Host: thecrownsgolf.org
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: INetSim HTTP Server
Connection: Close
Content-Length: 258
Content-Type: text/html
Date: Tue, 16 Aug 2016 23:27:27 GMT
```

```
C:\Users\test\Desktop>echo %computername%
MYHOSTNAME
```

Illustration A: WEBC2 Backdoor making connection to C2Server

[22]

```
GET /css/about.htm HTTP/1.1
User-Agent: Microsoft Internet Explorer Exelon MYHOSTNAME
Host: thecrownsgolf.org
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: INetSim HTTP Server
Connection: Close
Content-Length: 311
Content-Type: text/html
Date: Tue, 16 Aug 2016 23:04:23 GMT

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
  <div safe: KxAikuzeG:F6PXR3vFqffP:H balance></div>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Illustration B : C2Server sends encrypted string as part of a div tag. Backdoor program will decrypt the string, which contains a url to go to and download malware.

21 KA, Monnappa. "Understanding APT1 Malware Techniques Using Malware Analysis."

22 Ibid.

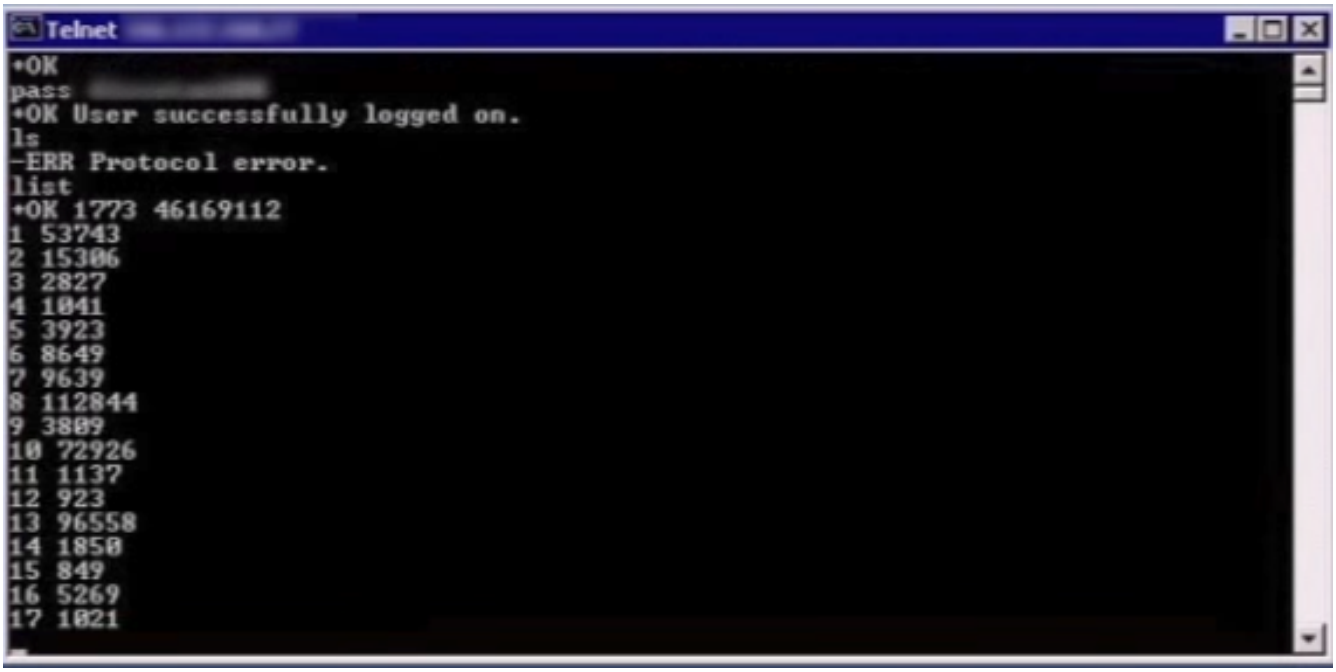

Illustration C: APT1 Attacker logs on to web mail using legitimate credentials, lists emails

After the attacker gained control of the system, APT1 would attempt to obtain usernames, passwords, and other credentials of unsuspecting users. They would do this by using publicly available privilege escalation tools (eg. cachedump, fgdump, pass-the-hash toolkit, pwdump7 etc), to dump password hashes, or encrypted passwords, decrypt them, and log in to legitimate user accounts.

Discovery and Capture

With full access to a company computer and the login credentials of legitimate users, the APT1 attacker does internal reconnaissance of the system: using shell commands or bash scripts, the attacker saves important data about the system (eg. what files are on the system, how the files or folders are arranged, what user permissions are required for what files, etc) and saves that information into a .txt file. The attacker then moves laterally through the system, finding connected shared resources and

23 *APT1: Exposing One of China's Cyber Espionage Units*. - Youtube Video

online portals that he or she now has access to. The attacker also maintains a presence by horizontally proliferating through computers on the network, installing new backdoors on multiple systems to assure that, if one backdoor is found and removed, APT1 will still have access to the computer network.

Exfiltration

Finally, once APT1 finds files of interest to them, the attacker or attackers will pack the files into an archive file, before sending it back to the C2 Server, and deleting the target computer's local archive file. If the attacker finds more login credentials of use to APT1 (or login credentials with more permissions), the attacker will once again escalate his or her own privileges, access new files, computers, and networks with the new permissions, and the cycle will begin again.

5. Attributing APT 1 to Unit 61398

Cyber security firm's Mandiant cast APT1 into public view, linking the hacker group's activities to a specific group in China's military: the Chinese People's Liberation Army (PLA) unit 61398. Mandiant argued the link in three ways. First, APT1's scale of operations, personnel expertise and apparent mission lined up exactly with Unit 61398. Unit 61398 is under the PLA's General Staff Department's (GSD) 3rd Department, which is in charge of signals intelligence (of which cyber security is a part). The unit, also known as the second bureau of this department, is tasked with computer network operations. The individuals they hire must have a good knowledge of English, as well as of operating systems[24]. The Project 2049 Institute reported in 2011 that Unit 61398's goal appeared to be to target the US and Canada, focusing on political, economic and military-related intelligence[25]. These targets and requirements line up well with APT1, a hacker group made up of English speaking individuals that, based on the sophistication of their malware and their ability to conduct multiple

24 Mandiant. "APT1: Exposing one of China's Cyber Espionage Units", 49
25 Stokes, Mark A., Jenny Lin, and L.C. Russell Hsiao. "The Chinese People's Liberation Army", 11

campaigns at once, is a very large scale and well-equipped organization, similar to that of a military bureau. Second, the location that the personnel are operating from, based off of telephone numbers used by attackers to set up fake phishing email accounts, physical addresses provided in domain registration and IP addresses used in software updates, matches the same city that Unit 61398 operates in. Over half of the HTML pages accessed through the C2 Server via WEBC2 back-doors to execute commands had domain names that were registered to either a Shanghai phone number from the Pudong district, or a Shanghai address. Although specific interaction between C2 Servers and infected computers were done through other infected computers, the path of HTTP requests and other communications could be traced back to a Shanghai IP address belonging to China Telecom (a Chinese telecommunications company). Shanghai is one of the largest metropolitan cities in Southern China, but the "Unit 61398 Center Building", the twelve-storie building the unit uses as its base of operations, is located in the Pudong district of Shanghai. Moreover, there is evidence that China Telecom has constructed fiber optic communication lines specifically for the Center Building. Third, specific individuals living in Shanghai with technical backgrounds within Unit 61398 have been matched to specific hacker personas involved in creating APT1 malware[26].

6. Trends in China and Unit 61398's Cyber Operations

Prior to Mandiant's report, works written in China on its cyber operations or policy were scarce, aside from vehement denials that China conducted cyber espionage[27]. However, indicators of China's ambition could be easily found in their Eleventh and Twelfth Five-Year Plans, published in March of 2006 and 2011 respectively. The five year plans, a series of development initiatives that guide the party's strategy for the five years after the plan is released, set wide-sweeping goals for the Chinese

26 Groll, Elias. "The U.S. Hoped"
27 Paganini, Pierluigi. "China Admitted the Existence of Information Warfare Units."

economic and social structures. The Eleventh Plan clearly states that “Industrial structure will be optimized and upgraded...by relying on enhancing independent innovation capability [and taking]...it as a national strategy”[28]. The Twelfth Plan echoes this, further adding that the Chinese government, in the five years following, wanted to “strengthen the R&D and industrialization of critical technological equipment”[29]. The United States, however, did have a cyber policy. In February 2011, the White House unveiled a new strategy aimed at combating the theft of U.S. trade secrets by hackers. Two months later, President Obama, who had stated many times that cyber security was an important agenda for his administration, issued a Cyber Security Legislative Proposal on establishing base standards of protecting critical infrastructure. When the proposal did not pass through Congress, he followed through by issuing an executive order in 2013 to put forward the standards developed collaboratively with the United States IT industry[30]. A few days later, Mandiant released its report on APT1. While information on Chinese hacking was available in Western media in bits and pieces, the report was the most blatant accusation of Chinese state-sponsored cyber espionage, backed up by considerable, quantifiable evidence. The Chinese government dismissed Mandiant’s conclusions as “baseless[31]”. Half a year later, however, a new issue of “The Science of Military Strategy”, an influential publication written by the Academy of Military Sciences of the PLA itself, was released in December 2013. Not only had this been the first edition since 2001 of the publication, but the 2013 edition contained a much more extensive view of Chinese military strategy rather than vague rhetoric, and notably included the first explicit acknowledgment of Chinese “network attack forces” that performed offensive cyber operations[32]. This admission was a watershed moment for China-US relations in cyber security. The transparency that “the Science of Military Strategy” offered in regards to China’s cyber security

28 (NDRC) People's Republic of China." The 11th Five-Year Plan”, 3
29 (NDRC) People's Republic of China." Full Translation of the 12th Five-Year Plan”, 1
30 The White House. “Securing Cyberspace”
31 Schwartz, Mathew J. "China Denies U.S. Hacking Accusations: 6 Facts."
32 Gady, Franz-Stefan. "Why the PLA Revealed Its Secret Plans for Cyber War."

strategy not only gave the United States insight into China's network operations, but also showed the United States that China was still interested in pursuing strategic stability in cyberspace[33]. Four large events followed: the US indictment on five Chinese hackers, the OPM breach, the 2015 US Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", and the 2015 Chinese Defense White Paper. First, the United States Department of Justice indicted five members of Unit 61398 connected with APT1, under 18 U.S. Code 1030, "fraud and related activity in connection with computers"[34]. However, the DOJ only charged the hackers under the sections of the statute dealing with gaining access to files of financial value, and not sections dealing with access to files of value to national security, even when there was evidence of both types of access. This deliberate decision to charge the hackers under one section but not another drew a distinction between military and industrial espionage. The decision, therefore, set a precedent that hacking into military and intelligence networks was in the realm of traditional spying and fair game, while hacking into corporate networks, the cyber-equivalent of industrial espionage, was not[35]. A year and a half later, however, the US Office of Personnel Management (OPM), found a breach of its computer networks dating back to March of 2014, tracing the intrusion to China[36]. The hackers broke into OPM's private network and got away with private data of over 390,000 government employees, used in background checks[37]. Then, around that time that the breach was found[38], President Obama issued yet another executive action, giving the executive branch the power to sanction individuals and entities responsible for carrying out cyber attacks against U.S. targets[39]. This executive order added new weight and authority to previous legislation and precedents – the United States executive branch was now able to

33 Ibid.
34 DOJ. ""U.S. Charges Five Chinese Military Hackers"
35 Ibid.
36 Krebs, Brian. "Catching up on the OPM Breach"
37 Ibid.
38 It is important to note that China's OPM breach was not the only cyber-assault uncovered around the time of the Executive Order. The attacks suffered by Sony Pictures Entertainment by North Korea and attacks on Target and other US companies also provided reason to issue the Executive Order.
39 Exec. Order No. 13694, 3 C.F.R. 3 (2015), 1

unilaterally and efficiently freeze Chinese assets of entities within China – state or military sponsored – deemed to be harming US critical infrastructure or engaging in commercial espionage through cyber-enabled means[40], showing the international community that, although conducting national security related cyber espionage was fair game, the United States could still very easily punish an individual (or group of individuals) for stealing intelligence information through cyber means. Only a month later, China released a new Defense White Paper, "China's Military Strategy", stating that the Chinese military had shifted their goal from "winning local wars under the conditions of informatization" to "winning informationized local wars". This change was based off the understanding that high-technology warfare was informationized warfare, and that informationized warfare would become the basic form of 21st century warfare. It went on to state that the Chinese military would give even greater weight to the application of information technology in all aspects of military operations, and that the key to a military victory was "information dominance"[41].

Finally, in September 2015, the two countries came to the negotiating table. During President Xi Jinping's visit to the White House on September 24 and 25, Xi and Obama came to a Cyber Agreement. This agreement, among other things, stated that the two countries would provide timely responses to assistance concerning malicious cyber activities, pursue efforts to promote appropriate international cyber norms, and refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property.

7. China's Unit 61398 Now and its Impact on Wider Cyber Trends

Today, Unit 61398 seems to have disappeared, its soldiers assumably sent to other military, private and intelligence units[42]. Moreover, commercial hacking in China has declined overall. An

40 Ibid, 2.
41 Fravel, Taylor. "China's New Military Strategy: "Winning Informationized Local Wars"
42 Sanger, David E. "Chinese Curb Cyberattacks on U.S. Interests".

intelligence report by FireEye, a cyber security company that acquired Mandiant a few years after the APT1 report, states that network compromises from February 2013 to May 2016 by Chinese hacking groups – state-sponsored or otherwise – dropped by 83 percent. Moreover, many recorded spear-phishing attempts from 2015-2016 are solely national security related, with targets ranging from Taiwan news organizations to Hong Kong dissidents[43]. Although this does not necessarily show a desire to completely stop conducting commercial espionage, this shows that China is making a concerted effort to abide by the agreement by separating national security targets from industry targets, and conducting cyber espionage in a far less overt way overall. While the lower volume of attacks may also be accompanied by a rise in sophistication of malware, causing attacks to be less voluminous but more focused and calculated (and harder to attribute), the sheer drop in raw numbers is enough to be optimistic. China has also actively taken part in the creation of other cyber norms, such as the "anti-hacking bill" portion of the G20 Leaders' Communique that upholds banning cyber-enabled theft of intellectual property[44], and two more rounds of cyber talks between the US Department of Homeland Security and the Chinese Ministry of Public Security[45].

8. Conclusion

While China has been accused of "attacking" the United States, China largely only conducts cyber espionage, stealing information from the United States through cyber means for its benefit. From Operation Aurora up until the Mandiant APT1 report however, China had been unscrupulously conducting cyber espionage on both the public and private sectors of the United States. A key example of its unapologetic, overt campaigns can be found in the actions of APT1, also known as China's People's Liberation Army 3rd General Staff Department's 2nd Bureau, Unit 61398. APT1 had been

43 Intelligence, Fireeye Isight. "REDLINE DRAWN: ", 12
44 Painter, Christopher. "G20: Growing International Consensus on Stability in Cyberspace."
45 DOJ. " First U.S.-China High-Level Joint Dialogue".

stealing from the entire spectrum of industries without covering its tracks from 2006, through Mandiant's 2013 report, until late 2014. Moreover, in the early 2000's, the US had no cyber norms to fall upon during breaches, the default action was to stay silent after a hack. In 2011, however, the Obama administration began making moves to create such cyber norms. Not only did the administration create a distinction between industrial and security cyber espionage, but also used that distinction when responding to the Mandiant report to indict five Chinese military personnel. Finally, after much posturing, the two countries have agreed on separating the two areas of cyber espionage, and have encouraged much of the international sphere to do the same. Moreover, Chinese state-sponsored hacks have declined dramatically – while this may increase the sophistication of the attacks, the United States will be better off dealing with a more elusive thief who gets away with less, than an overt, rampaging looter. Cyber security will still be an issue as long as the two countries continue to interact with each other on a political and economic level – while the development of these norms is only the beginning of a wide range of laws in the cyber security field, it is as good a beginning as any.

Sources:

1. *APT1: Exposing One of China's Cyber Espionage Units. Report. Mandiant. February 19, 2013. Accessed November 28, 2016. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.*

2. *APT1: Exposing One of China's Cyber Espionage Units*. Video. February 18, 2013. Accessed November 28, 2016. https://www.youtube.com/watch?v=6p7FqSav6Ho.

3. Branigan, Tania. "China Responds to Google Hacking Claims." The Guardian. 2010. Accessed November 28, 2016. https://www.theguardian.com/technology/2010/jan/14/china-google-hacking-response-dissidents.

4. Claburn, Thomas. "China Cyber Espionage Threatens U.S., Report Says." Dark Reading. November 20, 2009. Accessed November 23, 2016. http://www.darkreading.com/risk-management/china-cyber-espionage-threatens-us-report-says/d/d-id/1085047.

5. Exec. Order No. 13694, 3 C.F.R. 3 (2015).

6. "First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes." First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes | OPA | Department of Justice. December 2, 2015. Accessed November 28, 2016. https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0.

7. Fravel, Taylor. "China's New Military Strategy: “Winning Informationized Local Wars”." The Jamestown Foundation. July 02, 2015. Accessed November 28, 2016. https://jamestown.org/program/chinas-new-military-strategy-winning-informationized-local-wars/.

8. Gady, Franz-Stefan. "Why the PLA Revealed Its Secret Plans for Cyber War." The Diplomat. March 24, 2015. Accessed November 28, 2016. http://thediplomat.com/2015/03/why-the-pla-revealed-its-secret-plans-for-cyber-war/.

9. Groll, Elias. "The U.S. Hoped Indicting 5 Chinese Hackers Would Deter Beijing’s Cyberwarriors. It Hasn’t Worked." Foreign Policy. September 2, 2015. Accessed November 28, 2016. http://foreignpolicy.com/2015/09/02/the-u-s-hoped-indicting-5-chinese-hackers-would-deter-beijings-cyberwarriors-it-hasnt-worked/.

10. InfoSec. "Current Trends in the APT World." InfoSec Resources Current Trends in the APT World Comments. February 18, 2015. Accessed November 28, 2016. http://resources.infosecinstitute.com/current-trends-apt-world/.

11. Intelligence, Fireeye Isight. "REDLINE DRAWN: China Recalculates Its Use of Cyber Espionage." (n.d.): n. pag. *Fire Eye Isight Intelligence*. Mandiant, June 2016. Web. 23 Oct. 2016.

12. KA, Monnappa. "Understanding APT1 Malware Techniques Using Malware Analysis." Lecture.

13. Krebs, Brian. "Catching Up on the OPM Breach." Krebs on Security RSS. June 15, 2015. Accessed November 28, 2016. https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/.

14. Lewis, James A. *A Note on the Laws of War in Cyberspace*. Report. Center for Strategic & International Studies.

15. Lieberthal, Kenneth, and Peter W. Singer. "Cybersecurity and U.S.-China Relations." *Brookings 21st Century Defense Initiative*, February 2012. Accessed November 23, 2016. https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf.

16. "Mandiant APT1 (Comment Crew) Threat Response." Sophos Community. October 13, 2013. Accessed November 28, 2016. https://community.sophos.com/kb/it-it/118968.

17. Naked Security. "Operation Aurora Hack Was Counterespionage, Not China Picking on Tibetan Activists." Naked Security. 2013. Accessed November 28, 2016. https://nakedsecurity.sophos.com/2013/05/22/aurora-hack-espionage/.

18. National Development and Reform Commission (NDRC) People's Republic of China." The 11th Five-Year Plan: Targets, Paths and Policy Orientation". March 23, 2006. Accessed November 28, 2016. http://en.ndrc.gov.cn/newsrelease/200603/t20060323_63813.html.

19. National Development and Reform Commission (NDRC) People's Republic of China. "Full Translation of The 12th Five Year Plan." December 9, 2011. Accessed November 28, 2016. http://www.cbichina.org.cn/cbichina/upload/fckeditor/Full Translation of the 12th Five-Year Plan.pdf.

20. Paganini, Pierluigi. "China Admitted the Existence of Information Warfare Units." Security Affairs. March 20, 2015. Accessed November 28, 2016. http://securityaffairs.co/wordpress/35114/security/china-admit-cyber-army.html.

21. Painter, Christopher. "G20: Growing International Consensus on Stability in Cyberspace." US Department of State Official Blog. December 3, 2015. Accessed November 28, 2016. https://blogs.state.gov/stories/2015/12/03/g20-growing-international-consensus-stability-cyberspace.

22. Sanger, David E. "Chinese Curb Cyberattacks on U.S. Interests, Report Finds." The New York Times. June 20, 2016. Accessed November 28, 2016. http://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html.

23. Schneier, Bruce. "The Story Behind The Stuxnet Virus." Forbes. July 10, 2010. Accessed November 28, 2016. http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html.

24. Schwartz, Mathew J. "China Denies U.S. Hacking Accusations: 6 Facts." China Denies U.S. Hacking Accusations: 6 Facts. February 21, 2013. Accessed November 28, 2016. http://www.darkreading.com/attacks-and-breaches/china-denies-us-hacking-accusations-6-facts/d/d-id/1108750?

25. "SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts." The White House. January 13, 2015. Accessed November 28, 2016. https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

26. Stokes, Mark A., Jenny Lin, and L.C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." Project 2049 Institute. November 11, 2011. Accessed November 28, 2016. http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.

27. Sullivan, Dan. "Beyond the Hype: Advanced Persistent Threats." Trend Micro. Accessed November 28, 2016. http://la.trendmicro.com/media/misc/ebook-advanced-persistant-threats-and-real-time-threat-management.pdf

28. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage | OPA | Department of Justice. May 19, 2014. Accessed November 28, 2016. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

29. Yip, Ki Nang. "Spear-Phishing Case Study." InfoSec Resources SpearPhishing Case Study Category. Accessed November 28, 2016. http://resources.infosecinstitute.com/category/enterprise/phishing/spear-phishing-and-whaling/spear-phishing-case-study/.