Hacking between nations

Yuqing Lin

Binghamton University

Hacking between nations

After Stuxnet first attacks Iran's nuclear facilities, international cyberwar becomes problems and threats toward the U.S and China. Every year, the director of U.S national intelligence announces a threats assessment which analyzes and lists all threats toward the nation. In 2007, any cyber-related problems were not on the list. In 2009, cyber problems first appeared on the list but placed at the button of the list. In the past few years, however, cyber problems have vaulted to the top of the list (Zegart, 2015). Cyber problems have become serious problems not only for the U.S but also for many other countries like China and Russia. In the past five years, many countries have passed laws specifically regulate online activities. Although there are a series of conflicts between the two most advanced countries, China and the U.S in cyberspace, peace and more clear international regulations on cyberspace are the ultimate goal for both countries.

The first cyber-attack between China and the U.S occurred in 1999 during the Kosovo conflict. Chinese hackers respond to this event by forming up an organization called “红客联盟” which was translated into “red hat” hackers in English. In compare to “back hat” hacker, “Red Hat” hackers launch attacks to websites and company systems not for profits but revenge. After the U.S bombed the Chinese embassy in Belgrade, killing three Chinese reporters, Chinese patriotic hackers launch attacks to the U.S base websites and planted announcements-- “NATO’s brutal action” for days. After days of continual attacks, Chinese “red hat” hackers formed up the organization. Although the Chinese newspaper “people daily” published articles censured the attacks against the White House, Chinese “red hat” organization didn’t stop their attacks. “Web terrorism” as the term first occurred on the U.S newspapers and articles as responded to the series of attacks from this organization. However, the organization was dismissed in 2001 after launched cyber-attacks to the U.S in response to Chinese fighter jet collided with U.S fighter jet which was the last cyber-attack toward the U.S from Chinese patriot hackers.

After the “red hat” hacker organization dismissed, Chinese government recruited most of its members. In the past decade, the Chinese government formed a secret cyber army, unit 61398 which meant to defend the national network. However, many western countries claim that this secret army launch multiple DDOS (Distributed Denial of Services) attacks to websites such as the Chinese version of *New York Times and GreateFire.org.* This kind of websites often displease the Chinese government and discloses secrets that the Chinese government does not want anyone to know.

In 2013, the conflicts between unit 61398 and other western cyber defenses departments have further risen up. Many countries sued this unit for cyber invasions, stolen sensitive data as well as espionages. The Chinese government responded to this incident by saying

洪磊 2014 年 5 月 19 日表示：

中国政府一贯坚决反对并依法打击网络攻击行为。事实上，中国是网络攻击的主要受害国之一。针对中国的网络攻击、网络犯罪呈快速、逐年上升之势。根据中国国家互联网应急中心发表的报告，2012 年，7.3 万个境外 IP 地址作为木马或僵尸网络控制服务器参与控制中国境内 1400 余万台主机，3.2 万个 IP 通过植入后门对中国境内近 3.8 万个网站实施远程控制。在上述网络攻击中，源自美国的网络攻击数量名列第一。

中国社科院情报信息研究院院长张树华 19 日对《环球时报》表示，美国有关机构极力渲染“中国黑客”攻击，不乏夸大外来威胁、以从国会套取相关经费的盘算，是一种造

势。全球互联网尚是没有规则的社会，中国一直积极倡导互联网准则的设立，国际网络主权的概念已经提出。

In this statement, the Chinese government stated that they have been consistently cracking down cybercrimes and any cyber-attacks. They also claimed that the Chinese government did not launch any cyber-attacks, instead, they were doing their best to defend the country's network which was being invaded the most from the U.S. Since cyber-attacks are hard to track in real time and hard to find recodes as well as almost all countries decided to turn a blind eye to this kind of cyber-attack problems at international level, it’s hard to judge who is right.

However, the U.S and China are seeking peace on cyberspace by the U.S China agreement. In September 2015, President Obama and President Xijing Ping agree to fight against cyber enables thefts on business secrets as well as corresponding each other to fight against cybercriminals. However, the agreement does not cover cyber espionages which both countries consider as fair play (Denning,2017).

Speaking of cybercriminals, many countries successively passed cyber laws in the last decade to regulate online behaviors. China passed the *Chinese cybersecurity law* in 2016 which clearly states the leadership of the Chinese government and law enforcement. In China, all mobile services and internet providers have to obey Chinese law enforcement for investigating any cyber-related issues. Chinese policy has the right to access any cyber traffic information for investigations. If a cyber attack occurs, internet providers, as well as the victim company, have to report to the government immediately. This policy helps the Chinese government to.resolve any cyber-related issues and defense the national network in a much more efficient way. However, since the Chinese government has full accessibility to its national networks, users have almost no privacy protections online in China.

In comparison to China, the U.S government also has a specific law dealing with cyber attacks or related problems but in a different way. In 2014, the House passed the Cyber information sharing act of 2015 encourages private sectors to voluntarily share internet traffic information to government and law enforcement. This law also authorizes companies to monitor and implement defense software on their own network or information system. This law respects users' privacy by emphasizing the word "encourage" which means that private sectors have the right to refuse to correspond with government agents when dealing with cyber threats or cyber attacks. Thus the law still ensures users' privacy by only giving the government a certain level of accessibility online. However, since 85% of U.S basic infrastructures are run by private sectors, without giving the authorities to access internet traffic information in private sectors creates weakness and vulnerability in defending the country's networks (Zegart, 2015).

In conclusion, although there have been conflicts between China and the U.S on cyberspace in the past decade, fighting against cybercriminals as well as cyber enables thefts are commend agreement between these two nation. In the current environment of international cyberspace, with almost no regulations between nations as well as internet espionages become a comment practice between nations, the China-US agreement is a good beginning point of regulating cyber activities. In addition, many countries approach these problems in different ways. In China, the government taking the lead when fighting against cyber crimes and issues. In the U.S, the government is seeking a partnership between the government and private sectors by encouraging private sectors to share internet traffic information when dealing with cyber crimes. Clearly, although both countries' approaches have advantages and drawbacks based on policies in different countries with different conditions, fighting cybercrimes are command practices in both countries' policies.

References

中国红客联盟 – H.U.C. (n.d.). Retrieved from http://www.cnhonker.com/

中国人民解放军 61398 部队. (n.d.). Retrieved from https://baike.baidu.com/item/中国人民解放军 61398 部队/6029685?fr=aladdin

Denning, D. (2017). Hackers in China are conducting covert cyberattacks on the U.S. Retrieved from https://www.newsweek.com/chinese-hackers-cyberwar-us-cybersecurity-threat-67837

Karp, B. S., Paul, Weiss, Rifkind, & Wharton & Garrison LLP. (2016). Federal Guidance on the Cybersecurity Information Sharing Act of 2015. Retrieved from https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

TED. (Jun 29, 2015). Zegart,A :*Cyberwar* [Video file]. Retrieved from https://www.youtube.com/watch?v=JSWPoeBLFyQ