China's Economic Espionage

Stealing, Not Destroying

Reema Hibrawi

This paper seeks to examine the economic espionage threat to the national security of the United States from the Chinese government in the private and public sector. In this paper, economic espionage will refer to the unauthorized access and use of information by a foreign entity for strategic, tactical, or economic purposes.[1] The theft of trade secrets with the intent of an economic benefit by a foreign power, also falls under economic espionage.[2] The key research questions of this paper are: 1) Which U.S. targets are pursued by the Chinese government? 2) Why is China engaging in economic espionage against the U.S.? 3) What are the implications for U.S. national security?

This paper seeks to specifically discuss the economic, military, and security risks to U.S. national security. Economic risks include the loss of trade secrets and competitive advantage. Military risks include the theft of strategic information on operations, equipment, and personnel.[3] Security risks refer to infrastructure and government functions that rely on digital networks. The main focus will be on Chinese government network exploitation and attacks, as well as intellectual property theft.[4]

The analysis predicts that the Chinese government will continue to focus on persistent and aggressive economic espionage of the United States. This judgment is made due to the vast information from private security consulting and public intelligence agencies on attacks originating from China, and the current Chinese cyber strategy. It is less clear how the Chinese will continue to use economic espionage as a tool to maintain their economic growth. This uncertainty is due to the opaque and complex internal strategy on China's economic espionage. This may or may not be the main tool or focus for China's economic growth moving forward. Just as uncertain but highly probable is that the Chinese will continue to resist ratifying an international legal framework for cyber monitoring and security that is restrictive. This is based on failed negotiations in the past, and China's continued focus on maintaining legitimacy through its domestic and foreign policies.

RATIONALE

Historically, China is not known for its prowess in modernity. It has lagged behind the U.S. in innovation and resources in much of the 20th Century. China was inefficient, stagnant, and poor due to tight economic control and isolation by the state.[5] A shift occurred in the late 1970's, with the

[1] *Economic Espionage Act of 1996*: Title 18 Crimes and Criminal Procedure, Part I Crimes, Chapter 90 Protection of Trade Secrets, Pub. L. No. 104-294, 110 Stat. 3488 (Oct. 11, 1996), codified at 18 U.S.C. §1831. Passed as part of the *National Information Infrastructure Protection Act of 1996*.

[2] Charles Doyle, "Stealing Trade Secrets and Economic Espionage: An Overview of 18 U.S.C. 1831 and 1832," *Congressional Research Service* (July 25, 2014).

[3] Testimony of Larry M. Wortzel, "Cyber Espionage and the Theft of US Intellectual Property and Technology," before the House of Representatives, Committee on Energy and Commerce Subcommittee on Oversight and Investigations (July 9, 2013).

[4] Mark Lowenthal, *Intelligence: From Secrets to Policy*, 6th Edition (Sage/CQ Press, 2014), 456.

[5] Wayne Morrison, "China's Economic Rise: History, Trends, Challenges, and Implications for the United States," *Congressional Research Service* (October 9, 2014).

implementation of free market reforms[6] China continued to push for foreign direct investment (FDI) to this economic development.[7] It has become more influential as a result of improving its technology and intelligence capabilities.[8] This includes the modernization of its signal intelligence (SIGINT).[9] It has also shown space-borne capabilities in the form of anti-satellite (ASAT) tests in 2007 and 2013.[10] In the education sector, the state has emphasized science fields to continue this growth. There has since been an increase in Chinese students attending physics and computer science programs in U.S. universities and graduate programs.[11] This is seen as both an effort to modernize the population and develop cyber hacking capabilities for state use. The aim of modernizing into an information and industrial society has inspired the Informatization Plan of 2006.[12] One of the main goals is to close the digital divide.[13] China is on track to do just that as illustrated by its successful economic espionage on U.S. civilian and military organizations.[14] With its growing power as a world economy and increasing need for resources, Chinese intelligence and technology capabilities have improved to meet these demands.

IMPORTANCE TO THE U.S.

Along with these developments, the cyber domain is relatively new and unregulated, which makes economic espionage without consequences more prevalent. There are no legal frameworks to monitor cyber security at the international level,[15] and no precedent exists in policy at the domestic or international level.[16] The sovereignty of digital information is a point of contention between states like China and the U.S.; China prefers a more flexible interpretation which will not affect its domestic and political stability.[17] This has led to stalled agreements on international cyber security and norms.[18] The U.S. infrastructure is reliant on digital networks for its electricity, water, transportation, flight travel, and the economy.[19] Like most industrialized states, the U.S. is more vulnerable to economic espionage due to the level of integration between digital networks and national infrastructure.[20] Government social services like healthcare, industry, and commerce have transferred to digital structures. Besides the government, the public also is increasing its use and trust of digital technologies.[21] One third of the world is digitally connected and

---

[6] Beina Xu and Eleanor Albert, "The Chinese Communist Party: Backgrounders," *Council on Foreign Relations* (November 17, 2014).
[7] Jim Lewis, "China Economic Reform Timeline: Jim Lewis Blog," *Center for Strategic & International Studies* (December 11, 2014).
[8] Wayne Morrison, "China's Economic Rise: History, Trends, Challenges, and Implications for the United States," *Congressional Research Service* (October 9, 2014).
[9] Mark Lowenthal, *Intelligence: From Secrets to Policy*, 456.
[10] Ibid.
[11] Ibid.
[12] Amy Chang, "Warring State: China's Cybersecurity Strategy," *Center for New American Security* (December 2014).
[13] Zhongzhou Li, "China's Information Strategy and its Impact on Trade in ICT Goods and ICT Services," *UNCTAD Expert Meeting*, in Support of the Implementation and Follow-Up of WSIS: Using ICTs to Achieve Growth and Development (December 2006).
[14] Ibid.
[15] James Clapper, *Worldwide Threat Assessment of the US Intelligence Community* (January 29, 2014).
[16] Michael Hayden, "The Future of Things 'Cyber'," *Strategic Studies Quarterly* (Spring 2011).
[17] Amy Chang, "Warring State: China's Cybersecurity Strategy," *Center for New American Security* (December 2014).
[18] Ibid.
[19] White House Online, "International Strategy for Cyberspace" (May 2011).
[20] James Clapper. *Worldwide Threat Assessment of the US Intelligence Community* (January 29, 2014).
[21] Ibid.

this is likely to increase as more countries modernize and develop technology.[22]

For these reasons, the Director of National Intelligence (DNI) threat assessment of 2013 lists cyber security as a current and growing future threat to the U.S. and highlights China and Russia as the most pervasive and persistent in attacks against the U.S.[23] Chinese programs infiltrated over 1,295 computers in 103 nations.[24] They target U.S. national defense and national lab sites,[25] as well as cyber and technology firms.[26] These are substantial motivations for cyber security and protection from economic espionage as a key strategic initiative for the most recent Department of Defense (DoD) strategy of 2011.[27] The executive branch also lists cybercrime as a key focus in the White House International Strategy for Cyberspace.[28]

ANALYSIS

China has persistently denied existence of cyber units or economic espionage. It describes these claims as fictitious and baseless.[29] In 2010, of 614 known advanced persistent threats (APT) with distinct IP addresses attacking infrastructure systems, 100% were found operating out of Shanghai.[30] A prominent espionage unit, referred to as APT1, has instigated massive attacks and continues to steal huge quantities of information. Hundreds of investigations on economic espionage found that most activities originated in China and with government knowledge.[31] The extent of the attacks and resilience of the group suggest they have strong financial backing in addition to a sophisticated structure. With the highly monitored Chinese environment, it is unlikely the state is unaware. Evidence suggests the state must be supporting these activities because its attacks have not stopped.[32] The top industries include information technology, high-tech electronics, aerospace, public administration, and satellites and telecommunications.[33] Strong evidence shows that APT1 is Unit 61398 which is the People's Liberation Army (PLA) Third Department cyber espionage unit. Cyber activity originates in the same area where Unit 61398 is located.[34] The same structure, mission, and methodology exists in both units. The similarities between the two groups are difficult to ignore. The sophistication and investment in this espionage unit explains the assessment of China continuing persistent economic espionage against the U.S. as likely. The U.S. must continue to prepare for China's espionage activities.

Of exemplary importance, Unit 61398 targets civilian technology and proprietary information. Evidence shows that APT1 started stealing data as early as 2006.[35] Information that is targeted includes strategic plans, goals, calendar items, optimization

[22] Ibid.
[23] Ibid.
[24] A study undertaken by the University of Toronto in 2009, in Mark Lowenthal, *Intelligence: From Secrets to Policy*, 457.
[25] Mark Lowenthal, *Intelligence: From Secrets to Policy*, 457.
[26] Mandiant Online. "APT1: Exposing One of China's Cyber Espionage Units." A private security consulting service periodically releases cyber threat reports against the US and private sector companies.
[27] Department of Defense, "Department of Defense Strategy for Operations in Cyberspace" (July 2011).
[28] White House Online, "International Strategy for Cyberspace" (May 2011).
[29] Adam Segal, "Axiom and the Deepening Divide in U.S – China Cyber Relations," *Council on Foreign Relations* (October 29, 2014).
[30] Mandiant Online. "APT1: Exposing One of China's Cyber Espionage Units," 2013.
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Ibid.
[35] Mandiant Online. "Trends: Beyond the Breach, 2014 Threat Report."

processes, and joint venture information.[36] This suggests that the attacks are meant to understand how executives and decision makers think.[37] China is looking to gain influence through several means: economic, political, diplomatic, and military platforms. China-based attacks steal ideas and the process to developing those ideas. The cost for these activities is minimal. Risk is low and gaining access to large quantities of information can be done quickly by manipulating networks, e-mail, and digital downloads to external storage devices.[38] Detection is difficult over networks because the location of the perpetrator can also be masked.[39]

U.S. private sector firms, academia, and private citizens of various countries are prime targets for China. Evidence shows that Marathon Oil, ExxonMobil, and ConocoPhillips were hacked in the summer of 2008 and lost data detailing the quantity, value, and location of oil discoveries around the world. The loss of such data per company ranges in the millions of dollars.[40] The Chinese are the most pervasive and relentless actors in economic espionage, besides Russia.[41] The U.S. is the leader in technological and economic development which makes it a target by its competitors, and especially China.[42] Information and stolen data is provided to Chinese state owned enterprises which cuts costs, research and development timelines, and improves the competitive edge of these industries.[43] The economy as a whole can also be damaged by the compromise of private sector trade secrets, which can affect job creation, profits, and future innovation.[44]

Military economic espionage has targeted several DoD weapons systems including ballistic-missile defense systems, Black Hawk helicopters, and combat ships.[45] Military operations and the individuals involved are compromised when military documents are stolen. China seeks information on the manufacture of weapons and their systems to replicate and counter their designs. This is an effort to modernize the state and improve its military capabilities. Evidence of this is seen through its anti-satellite tests to counter U.S. military use of satellites for offensive behavior.[46] More specifically, evidence has also shown that Chinese hackers stole classified information in February 2012 about the technology behind the F-35 joint strike fighters.[47]

CHINESE STRATEGY

Currently, China's cyber strategy is an extension of its national security strategy. This

---

[36] Ibid.
[37] Ibid.
[38] "Foreign Spies Stealing US Economic Secrets in Cyberspace," Counterintelligence Security, Office of the National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (October 2011).
[39] Ibid.
[40] "Cybersecurity: A list of significant cyber events since 2006," Center for Strategic and International Studies (April 2015).
[41] "Foreign Spies Stealing US Economic Secrets in Cyberspace," Counterintelligence Security, Office of the National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage*, *2009-2011* (October 2011).
[42] Ibid.
[43] Testimony of Larry M. Wortzel, "Cyber Espionage and the Theft of US Intellectual Property and Technology," before the House of Representatives, Committee on Energy and Commerce Subcommittee on Oversight and Investigations (July 9, 2013).
[44] "Foreign Spies Stealing US Economic Secrets in Cyberspace," Counterintelligence Security, Office of the National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage*, *2009-2011* (October 2011).
[45] Ibid.
[46] Mark Lowenthal. *Intelligence: From Secrets to Policy*, 457.
[47] "Cybersecurity: A List of Significant Cyber Events Since 2006," Center for Strategic and International Studies (April 2015).

is to maintain legitimacy of the Chinese Communist Party (CCP). It is likely China will resist ratifying an international legal framework to maintain legitimacy. The CCP maintains legitimacy by ensuring domestic stability, military modernization, economic growth, and territorial integrity.[48]

In order to become a better innovator of information and industry, Chinese domestic policy needs to focus on technology and science and the current leader in both technology and innovation is the U.S. It follows that China's main targets are U.S. private companies, military, and government. Chinese economic espionage serves several purposes: political, military, and economic.[49] China is simultaneously maintaining legitimacy, anticipating cyber conflict, and growing its economy. For these reasons, it is likely that China would use economic espionage as an integral tool for economic growth and other domestic policy objectives. Understanding that China seeks economic espionage for several reasons, mostly to maintain power and economic growth, is important in anticipating future U.S. targets.

It has been argued that China is using economic espionage solely for military offensive strategy or economic growth. Either premise is too simplistic and overlooks the Chinese style of governance in the last century. As previously mentioned, a major objective of the CCP is to maintain its legitimacy. All policies, both domestic and foreign, are shaped by this priority of self-preservation.[50] Because a major objective of the CCP is to maintain its political legitimacy, it is prone to using economic espionage to meet both objectives—military prowess and economic development, as both are important contributors to CCP's legitimacy. The combination of military and economic growth is a stronger method of maintaining authority than either alone. The CCP has been in power for over eighty years, and has remained in power by maintaining political and economic stability.[51] Chinese President Xi Jingping has also emphasized the importance of cyber technology in China's pursuit of power through the 2006 Informatization Plan, and in recent national security law drafted specifically to establish "systems of cyber and information security and national cyber sovereignty."[52] This law highlights the importance of cyber technology and security for Xi and the CCP in maintaining legitimacy. Economic espionage is likely to continue to be a tool for that end.

The U.S. does not have complete information about the motivations and patterns of Chinese economic espionage. This is because not every Chinese economic espionage attack has been successful or detected.[53] The limitations of the CCP cyber strategy is also unknown. Few public

---

[48] "Foreign Spies Stealing US Economic Secrets in Cyberspace," Counterintelligence Security, Office of the National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (October 2011).

[49] James Lewis and Simon Hansen, "China's cyberpower: International and Domestic Priorities," *Australian Strategic Policy Institute* (November 12, 2014).

[50] Amy Chang, "Warring State: China's Cybersecurity Strategy," *Center for New American Security* (December, 2014).

[51] Beina Xu; Eleanor Albert, "The Chinese Communist Party: Backgrounders," *Council on Foreign Relations* (November 17, 2014) ; Amy Chang, "Warring State: China's Cybersecurity Strategy," *Center for New American Security* (December 2014).

[52] "China defines overall national security outlook in draft law," *People's Daily* (April 20, 2015).

[53] Testimony of Dr. Larry M. Wortzel before the House Armed Services Committee, "China's Military Modernization and Cyber Activities," *Strategic Studies Quarterly* 8, no. 1: 3-22. *International Security and Counter Terrorism Reference Center* (Spring 2014).

documents exist on this secretive program.[54] There are assumptions that the CCP would not steal information that could be seen as an act of war. Yet there is no evidence from the CCP or Xi if this assumption is accurate. The CCP may have its own unspoken rules about what to collect and what not to prioritize. This standard may be an understanding within the top leadership culture, not documented officially, and also kept secret.

The highest priority for the Chinese government is maintaining domestic stability. If this were to change, China would be forced to focus on domestic rather than foreign policy. It is not likely that espionage acts would stop, but the attacks would decrease as focus is shifted to the domestic sphere and managing censorship or internal attacks. If China agrees to ratify an international legal framework, this might also alter the structure of China's economic espionage units. China still believes it needs the information provided by its economic espionage units to modernize and grow, so again economic espionage would continue.

CONCLUSION

The aim of Chinese espionage has historically been to gain an economic edge over its competitors. Because espionage has been a relatively low-cost method to obtain important technology for economic development, and because China needs these technologies at its current level of development, it is likely that such economic espionage will continue. On the other hand, this paper has found that China has not used its stolen information for military aggression, although it targets military intelligence in both nuclear and satellite classified information.[55] It is unlikely China will have a major cyber-attack on U.S. infrastructure that would cause wide scale disruption.[56] It is also unlikely China will use cyber warfare in the next three years unless it believes its vital interest, the political legitimacy of the CCP regime, is violated.

FURTHER READINGS:

Chang, Amy. "Warring State: China's Cybersecurity Strategy." *Center for New American Security*. December, 2014.

"Cybersecurity: A List of Significant Cyber Events Since 2006." Center for Strategic and International Studies, April 2015.

Mandiant Online. "APT1: Exposing One of China's Cyber Espionage Units." https://www.mandiant.com/resources/mandiant-reports/.

Segal, Adam. "Axiom and the Deepening Divide in the U.S – China Cyber Relations." *Council on Foreign Relations: Net Politics*. October 29, 2014.

White House Online. "International Strategy for Cyberspace." May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Wong, Edward. "For China, Cybersecurity is Part of Strategy for Protecting the Communist Party." *The New York Times*. December, 3, 2014.

[54] Amy Chang, "Warring State: China's Cybersecurity Strategy," *Center for New American Security* (December, 2014).
[55] Ibid.
[56] Adam Segal, "The code not taken: China, the United States, and the future of cyber espionage," *Bulletin of the Atomic Scientists* (2013).

Reema Hibrawi is a Syrian-American with an international background having lived and studied in the Middle East, Europe, and the US. Her educational background includes a Bachelor's of Science in Business Administration with a focus in HR, and currently is pursuing a Master's of Arts in International Relations at New York University. Currently a corporate planning intern at the Council on Foreign Relations (CFR) her career goals include continuing to work on international affairs and project management within civil society and international organizations, or think tanks with a concentration on post-conflict development, and diplomacy and civil society.