Loyola Marymount University

The Potential of China’s Five-Year Plan in Protecting American Assets

Computer Science

Milla Penelope Markovic

Mentor: Professor Matthew Miller

Abstract: As technology and internet use have grown, complaints from internet crime victims as well monetary losses due to internet crime have increased as well. Law enforcement have identified some of the top threats in cyber space to be those posed by nation-states, specifically China. Considering the power that the United States holds on the world stage and the knowledge law enforcement has about the issue of cyber attacks on the United States by China, the question of why the country continues to experience such attacks becomes increasingly significant. Furthermore, how can China’s Five-Year Plan, along with United States’ knowledge of its past attacks be used to better understand China’s motivations and combat China’s cyber threat? The proposed research will help answer this question by analyzing past cyber attacks attributed to China along with the Five-Year Plans corresponding to the time of these attacks. It will also analyze China’s most recent Fourteenth Five-Year Plan to identify potential targets.

As technology and internet use have grown, especially in recent years, complaints from internet crime victims as well monetary losses due to internet crime have increased as well. Within the last five years, the FBI’s Internet Crime Complaint Center has received 2.67 million complains with $18.7 billion in total losses. (FBI 7) In fact, the Internet Crime Complaint Center, or IC3, received a "record number of complaints” in 2021 with 847, 376 complaints reported and “potential losses exceeding $6.9 billion.” (FBI 3) With the growing number of crimes committed on the internet, addressing this problem has become increasingly important.

While there are many different types of crime committed on the internet, from extortion to personal data breach, each committed by different individuals, law enforcement have identified some of the top threats in cyber space to be those posed by nation-states. In a statement given by FBI Assistant Director of the Cyber Division, Bryan A. Vorndran, to the House Judiciary Committee, he explains that some of “[t]he most significant nation-state threats [the United States] faces are those from China.” (Vorndran) In fact, when listing the “Top Cyber Threats” for 2022 and beyond, nation-state threats were the first topic discussed by Vorndran, suggesting that nation-states such as China are a primary worry for law enforcement and cybersecurity agencies. Although awareness of nation-state threats has increased in recent years, law enforcement agencies have been aware of the threat nation-state actors pose for decades. The United States is under cyberattack so often that “the FBI is opening a new China-related counterintelligence case about every 10 hours” according to FBI Director Christopher Wray in a 2020 remark at the Hudson Institute.

Considering the power that the United States holds on the world stage and the knowledge law enforcement has about the issue, the question of why the country continues to experience attacks becomes increasingly significant. This in part seems to be due to manpower differences between China and the United States. As explained by Charlie Mitchell in his book *Hacked: The Inside Story of America’s Struggle to Secure Cyberspace*, “China face[s] no manpower limits… far from the case in the United States.” (209) If the United States has fewer resources than China in terms of cyber manpower, the United States must find an alternative method to address the issue, such as identifying the largest targets for cyber-attack in order to protect these targets. Fortunately, the Chinese government publishes its political and economic goals publicly every five years in their Five-Year Plans. This leads to the question: how can China’s Five-Year Plan, along with United States’ knowledge of its past attacks be used to better understand China’s motivations and combat China’s cyber threat?

Since as early as 1949, when the Chinese Communist Party began to rise, one of China’s primary goals has been to become a global superpower according to Constance S. Uthoff in her book *Cyber Intelligence: Actors, Policies, and Practices*. In order to achieve this goal, China’s primary strategy has been to become an economic superpower through top technologies. While countries such as the United States have spent decades of time and large amounts of money on research to develop new technologies that have resulted in economic power, China has used espionage and intellectual property theft to attain such goals. As stated by FBI Director Wray in a 2020 speech, China must grow and has grown economically and technologically by “any means necessary” to reach its goals. While American citizens may not feel that China’s cyber threat directly impacts him or herself, “[i]f you are an American adult, it is more likely than not that China has stolen your personal data,” (Wray) likely through hacking large companies that store Personally Identifiable Information, or PII. Examples of such attacks include the hack of Anthem, a health insurance company, and the federal government. Not considering the losses of American citizens’ PII, it is estimated that “the annual cost to the U.S. economy of counterfeit goods, pirated software, and theft of trade secrets is between $225 billion and $600 billion” with China as “the world’s principal infringer of intellectual property.” (FBI 1) This further illustrates the threat that China’s cyber-attacks pose as well as their incredible damage to the United States.

In order to study how China’s Five-Year Plans may provide insight into the attacks that the United States is experiencing, a literature review will need to be conducted to ensure a full understanding of the role China’s Five-Year Plans play in government as well as China’s history of cyber-attacks. In addition, related tactics used by the Chinese government to obtain US trade secrets, such as Talent Programs, should be reviewed. After a thorough understanding of Chinese government goals and tactics is established, a literature review of the US and China’s role in cyberspace will also need to be conducted to gain a better understanding how technology has shaped and continues to shape how the two countries interact in cyberspace. The next step of this research would be a literature review on past research conducted on the topic of US and Chinese cyber relations. Once a solid foundation of background knowledge has been established, a study of past cyber-attacks attributed to China will be conducted. These attacks will then be compared to their corresponding Five-Year Plan based on time of attack, so an analysis searching for correlation or causation can be established. Finally, an analysis of recent cyber-attacks attributed to China will be conducted along with an analysis of China’s Fourteenth Five-Year Plan, published in 2021.

The expected product of this research is a paper illustrating correlations between past China’s Five-Year Plans and cyber-attacks on the United States attributed to China. In addition, this paper would provide an analysis of China’s current Fourteenth Five-Year Plan which would be used to provide predictions on the most at-risk industries and institutions. This would allow those highly at-risk to get a better understanding of how and why they are at risk of a cyber-attack providing the United States with a method of preventing cyber breaches despite less cyber manpower in comparison to China.

As Mitchell succinctly describes, past hacks have been “a wake-up call to America and the West, who have been far too complacent in the face of the demonstrated and growing cyber threat posed by Russia, China, Iran, as well as North Korea… Our national security is not only dependent on physically safeguarding the American people, but also developing the means to prevent a rogue nation or a terrorist group from launching a cyberattack that results in hundreds of millions of dollars in damage or the loss of life.” (169) The threat that China poses has and continues to increase as the country obtains new technologies, develops new tactics, and gains access to more manpower. However, the United States has not lost and has the ability to defend such attacks despite less manpower with a thought-through system developed around China’s specific goals and methods published by the government publicly. An analysis and research on China’s Five-Year Plans in regards to their impact on cyberspace could directly serve the United States by providing the government, cybersecurity agencies, and average Americans the knowledge to combat attacks. “[T]he U.S. political system and stakeholders from multiple industries, academia, civil liberties groups, and elsewhere must formulate policies that get beyond reactive scrambles to avert disaster in the moment,” (Mitchell 270) so that American assets and citizens might be protected.

**Proposed Budget**

No additional materials are needed to complete this research. Only a personal laptop and resources available through the LMU library will be used. 8 hours a day for 16 weeks at a wage of $15 per hour would total to $9,600.

**Proposed Timeline**

|  |  |
| --- | --- |
| Time: 4 months Total | Task |
| 2 Weeks | Literature Review: China’s Five-Year Plans; Chinese government (currently and historically); China’s Talent Programs |
| 4 Weeks | Literature Review: United States’ role in cyberspace; China’s role in cyberspace; US and Chinese cyber relations |
| 5 Weeks | Study/analyze past cyber-attacks attributed to China and past Five-Year Plans. |
| 2 Weeks | Study/Analyze China’s Fourteenth Five-Year Plan and cyber attacks during or after 2021. |
| 1 Week | Conduct further research to fill any gaps. Compare findings to others’ research. |
| 2 Weeks | Write results. |

Works Cited

“China: The Risk to Corporate America.” *FBI*, Federal Bureau of Investigation, 4 Oct. 2019, https://www.fbi.gov/file-repository/china-risk-to-corporate-america-2019.pdf/view.

“Director's Remarks to the Boston Conference on Cyber Security 2022.” *FBI*, FBI, 1 June 2022, https://www.fbi.gov/news/speeches/directors-remarks-to-boston-conference-on-cyber-security-2022.

“FBI Internet Crime Report 2021.” *FBI*, Federal Bureau of Investigation, https://www.ic3.gov/Media/PDF/AnnualReport/2021\_IC3Report.pdf.

Mitchell, Charlie. *Hacked: The Inside Story of America’s Struggle to Secure Cyberspace*. Rowman & Littlefield, 2016.

“Oversight of the FBI Cyber Division.” *FBI*, Federal Bureau of Investigation, 29 Mar. 2022, https://www.fbi.gov/news/testimony/oversight-of-the-fbi-cyber-division-032922.

“The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States.” *FBI*, Federal Bureau of Investigation, 7 July 2020, https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

Uthoff, Constance S. *Cyber Intelligence: Actors, Policies, and Practices*. Lynne Rienner Publishers, Inc., 2022.