WHY IS CHINA THE MOST DANGEROUS CYBER ADVERSARY FACING THE UNITED STATES?

Jason Rivers | Cyber Warfare Paper Project

March 4th, 2024

Old Dominion University
POLS 426 Cyber War

Introduction

For the last few decades, and for the foreseeable future, China stands not only as the largest cyber adversary facing the United States, but also as a clear geopolitical rival on the world stage. Not only does China rival the U.S. economically and politically, but they've also been making strides in their military and cyber capabilities to the point of being able to indirectly impact infrastructure of not only the U.S., but our allies as well. Geopolitically, they've been making moves not only to increase their international influence, such as targeting key U.S. assets and allies, utilizing a combination of physical, economic and political pressure, as well as using state-sponsored, and independent cyber groups to apply additional pressure. Technologically, they've also been targeting U.S., and allied research and technical institutions, and innovations seeking to manipulate, copy, and outright steal designs and data to advance their own means via cybercrime, espionage, and coercion of individuals abroad. Due to all these factors and more, I firmly believe that China is most dangerous cyber adversary currently facing the United States.

Brief Overview of US-Chinese Relations & the Developing Rivalry

Due to the introduction of this paper, you may be asking yourself "Why would China be the biggest rival to the U.S? Wouldn't that be Russia?" To an extent, you would be correct. Historically for the last century Russia (the former Soviet Union) has directly and indirectly been the largest geopolitical rival facing the U.S, with China being an ally of the former Soviet Union. This was before the Sino-Soviet split in the early 1960's where political differences, and numerous conflicts of interest led both nations to an impasse politically, economically, eventually led to an "undeclared open military conflict" in 1969 (Hart, 1983). Eventually the U.S. would swoop in to establish political and economic ties with China, with one of the earliest, largest political relations being dubbed "Ping-Pong Diplomacy" in 1971, and former President Nixon's visit in 1972. Continuing positive relations with China into the following administrations, former President Carter then worked to strengthen ties to China, not only fully recognizing them diplomatically, but also acknowledging the "One-China Policy" and effectively severing ties with Taiwan, an independent country off the coast of China that their government has historically claimed as part of their own territory since the end of World War II (Wiseman, 2015).

This brief, surface level history lesson was not meant to summarize over 50 years of political history into one paragraph, but rather highlight two main points: the U.S. historically has seen China as a more of a political, situational ally than a geopolitical rival, and that the fact of Taiwan's existence as an independent sovereign state to this day remains as an important agenda of the Chinese government, something I will expand on later. With US-Chinese relations so positive thanks to their shared animosity with the Soviet Union, how did the situation deteriorate between the two states to the point of an open-rivalry?

With the decline and eventual fall of the Soviet Union in 1991, this opened the doors for the US to solidify itself as a dominate world leader, with Chinese leaders also taking advantage of the fall to establish newly renewed diplomatic ties with the newly established states, and Russia itself. Throughout the 90's and well into the 2000's Chinese leaders continued to work on diplomatic relations, and more importantly economic ties throughout Asia, and Eurasia. This eventually led to the Chinese seeing the US more as a competitor, limiting their influence in the Pacific, and forcing them to focus efforts on overland relations for the moment (Standish, 2021).

China was able to weather the financial crisis of the late 2000's thanks to a combination of well-established economic ties throughout Central Asia, and the access to relatively cheap manufacturing labor and a resilient, growing market that international companies had in China following the financial crisis. Throughout the 2010's and into the 2020's China further spread its influence throughout Asia, and into the Pacific, causing tension throughout the region with regional powers, and as a result the U.S itself (Standish, 2021). All this time, China was not only developing itself as a political and economic rival to the US, but as a rival in the realm of cyberspace as well.

Chinese Focus on Cyber Capabilities

As we've gone over in class, China first began to invest in its cyber capabilities following the Gulf War. The U.S dazzled the world with its combined approach of utilizing support technology, communication, planning, and combined military might of an allied force. They realized that if they were eventually on the receiving end of another Gulf War-style conflict, they would have almost no chance of victory. As a result, they began planning, reforming, and developing their military to include more advanced technology such as information technology, with an emphasis on cyber capability. They focused on this so much so in fact that in 2013 the Chinese military publicly stated that "cyberspace has become a new, and essential domain of military struggle" (Jinghua, 2019).

They were entirely correct; the increased use of cyberspace and the internet has become intrinsically linked to how we live our lives today. Social media, news, work, technology around the house, even the class for which I'm writing this paper for, and the ability to read this paper right now are all thanks to cyberspace. Cyberspace and information technology as a whole are one of the greatest tools mankind has ever gifted itself, but just like any other tool it can be used or abused depending on who uses it, and how.

Part of how China has been so successful is not only their willingness to use it, but some of the methods of how they use it as well. China has a well-established history, and system of utilizing proxies for many of their cyber warfare operations. From 1994 to 2003, the Chinese government appeared to allow a number of proxy cyber attackers to "do business" against their rivals unabated. From 2003 to 2013, they appeared to be providing them support, and the issue has only gotten worse over time (Canfil, 2022). Over time, the use of proxies has only risen, with support from their government being highly suspect; the advantage of using proxies is that it gives the government utilizing them plausible deniability. They can simply claim they were wayward citizens or rogue agents, and their actions do not reflect the government's stance on cyber warfare, no matter how advantageous or successful their operation(s) were. This has been the case with multiple groups and APT's associated with attacks against some of their geopolitical allies within their own sphere of influence.

As we discussed before, China has been looking to spread its influence throughout Central Asia, and eventually into the Pacific region. One very clear target within the past few years has been the Republic of the Philippines, an archipelagic nation in Southeast Asia just south of Taiwan. Over the past decade, China has attempted to exercise increased influence over the nation, not only influencing it politicly, but also buying up many electrical assets within the nation (Swigart, 2023), and investing heavily into many businesses and corporations. While seeking to direct control over several key aspects of the nation, they have also been using cyber-attacks, and information warfare to further put pressure on the economics, society, and governmental bodies within the country.

The Influence of Cyber Warfare on the Philippines

The Philippines are unfortunately not known for their robust cyber capabilities, which leaves them open to attack from a more sophisticated adversary like China. Chinese agents have launched several notable cyber-attacks that have impacted, infiltrated, and influenced entities throughout Philippine economics, and government. This has included but is not limited to disinformation campaigns, data breaches, espionage and theft of intellectual property, personal data theft, and denial of service to many businesses within the country (Campbell, 2023). Part of the disinformation campaign mentioned before was a campaign of Pro-Chinese influence throughout social media in the country in 2020, before the country's election cycle just 2 years later. This election cycle saw Ferdinand "Bongbong" Marcos Jr., a political figure who repeatedly throughout his campaign praised China and mocked the US, assume the office of President. It can be argued that part of this Pro-Chinese influence was to not only impact them as a clear rival to China in the Pacific, but also to work to undermine U.S.-Philippine relations as well.

The Philippines has been one of the longest-standing relationships the U.S. has within with Indo-Pacific region, dating back officially to 1951. Creating a rift between the two allies, and causing Philippine leaders to request the U.S. withdrawal of stationed forces and support would not only vastly undermine the U.S. presence within the Pacific, but it would also harm our economy, and put Taiwan is a much more precarious position than it is already in. Chinese cyber warfare capabilities have repeatedly targeted Philippine entities with the purpose of not only causing economic, social, and political strain, but also to further the direct influence they have on the country through the use of cyber-crime, disinformation, and Advanced Persistent Threats (Campbell, 2023). This dangerous combination of direct political or economic influence coupled with indirect cyber influence can successfully influence a target nation, as well as weaken their attempts at combatting it in any notable capacity. By itself, China's cyber warfare capabilities are threatening to say the least but coupling that with the geopolitical pressure they extort within their own sphere of influence, and it becomes a dangerous combination that can be used again and again overtime. This can be seen not only with the Philippines, but with China's main target in the Indo-Pacific region, Taiwan.

Chinese Cyber Warfare against Taiwan

As we discussed before, Chinese focus on and obsession over Taiwan has gone back decades. From their "One China policy" claiming the island nation as part of their own country to desiring the island nation's technological and processing assets regarding semiconductors and computer chips (Kelter, 2022) and disrupting the delicate balance of power in the region, China's obsession over the island is not without merit. The small island nation is a key player in the Indo-Pacific, and a huge investment that the U.S. wishes to protect, albeit while only recognizing them in an unofficial capacity. Thanks to U.S. backing of Taiwan, as well as the isolated nature of the island, this leaves physical claims on the island off the table for now, which has led to a focus on using asymmetric cyber warfare to apply pressure to them.

With Taiwanese elections beginning on January 13, 2024, cyber warfare against Taiwan was clearly focused on all aspects surrounding this pivotal election cycle. Beginning in the latter half of 2023, and into the next year, cyber-attacks targeting Taiwanese infrastructure, government, and technology increased over 3000% compared to the normal rate of cyber-attacks against them according to a report from security firm Cloudflare (Pacheco et al., 2024). While not all could be traces back to Chinese services or attackers, many in fact were, and there wasn't much effort put into hiding that fact. The purpose of the massive cyber-attack campaign was clear as day: to disrupt Taiwanese services, steal as much data as possible, and to cast a shadow of doubt on not only governmental bodies but against Taiwanese officials that go against Chinese interests (Miller & Gedeon, 2024). Their lack of interest in hiding or masking the source of the attacks was clearly meant to intimidate not only Taiwan, but the U.S., and any other international body that seeks to go up against China and their interests.

I think this is really the essence of cyber warfare from China's perspective; every aspect of it, from the attacks themselves to the flexibility of what can be done, even to the act itself and displaying who did it can be used to apply pressure to an adversary. They not only utilize it as a form of active campaigning against their rivals, whether it be asymmetrical information warfare and cyber-attacks on U.S infrastructure or other rivals (Xu & Lu, 2021), but they also use it to dissuade cyber-warfare tactics and resistance against them. It basically tells anyone, like the Philippines, Taiwan, the U.S., and any other geopolitical rivals "Look what we did to them. If you stand against us, this will happen to you." They can not only focus direct and indirect cyber-attacks on a nation, but they can also launch campaigns espionage, or appropriation of technologies as well. This has been seen throughout Europe, Taiwan, and of course throughout the U.S.

Chinese Campaigns to Steal Technological Assets & Conduct Espionage

China's quest to secure parity with the United States has been going on for decades now. To an extent, they have accomplished that goal, becoming the main economic rival of the U.S. on the world stage. Militarily, it can also be argued that they are our equal, albeit within their own sphere of influence. Thanks to their advancing cyber capabilities, and active cyber warfare campaigns, they can make up for some shortcomings and keep propelling themselves forward in this endeavor. One of the biggest steps they've taken is to secure their own technological development, although this has been defined by both domestic and international theft of intellectual properties (IP) and assets from foreign businesses, and governments.

Ever since the 2000s-era economic recession, the Chinese economy has exploded, growing exponentially in the last decade. This ended up attracting thousands of businesses, and their intellectual properties along with them. These businesses are attracted not only by the new, vibrant market for sales that China offers, but by the affordable, plentiful manufacturing labor they find there as well. Once in the market or at least doing business with in it, Chinese businesses and firms seek to steal data, trade secrets, or reverse engineer assets and technologies for their own use. A widely used way they do this via joint ventures; an international company seeking to do business within China cooperates with a Chinese firm to sell and promote their product or service within the Chinese market. For this to happen however, the Chinese firm must be given access to the IP and technology of the product or service as per Chinese law. This trend of joint venture sharing gives Chinese firms and by extension, the government, access to technologies that could normally be outside of their ability to research or develop. This can and has led to Chinese businesses developing their own version of a technology or product and replicating to sell on the international market after they cut ties(O'Conner, 2019).

While not all Chinese firms and businesses are subject to sharing IPs and technological assets over to the government, once the transfer of information is "requested", they are forced to acquiesce (O'Conner, 2019). These newly obtained informational assets can be reverse engineered, and developed to further the nation's own technological, economic, military, or cyber warfare capabilities without having to waste resources. The long, arduous process of research and development (R&D) is cut down, and they're free to reap the benefits of reduced production and implementation costs (Scissors, 2021). This poses a new question however: what happens when an entity such as a government, or company with no desire for a joint venture has an IP, asset, or technology they wish to acquire?

Since joint ventures, and more economic-based solutions are off the table, the Chinese government seeks to utilize a mix of its own cyber-warfare tactics such as espionage, as well as infiltration, and talent acquisition. China has a prolific history of being tied up in, if not clearly orchestrating many corporate, and international espionage operations throughout economic, political, academic, and technological facilities around the world. Just within the U.S, a report from the Department of Justice in 2021 asserted that 80% of economic-espionage cases that they were able to identify and discover could be linked back to China (Scissors, 2021).

There are cases of Chinese intelligence agents attempting to hire, or coerce researchers, and staff members of many military, research, and academic institutions to hand over information, as well as potentially blackmailing Chinese-born foreign exchange students and professors to gather information from their facilities of study (Hannas & Tatlow, 2021). In some cases, Chinese agents utilize front companies, posing as shopkeepers or restaurateurs as a disguise to conduct their information gathering, and espionage operations. These espionage operations aren't just limited to coercion or blackmail, they can include cyber-attacks, and physical intrusion attempts to gather data from otherwise inaccessible locations, like governmental databases. Of course, this is not to say that other countries have never done the same. Most modern countries have active espionage operations ongoing against both enemies and allies whether they admit to it or not. With that being said, Chinese espionage and technology theft operations are at an unprecedented scale with no end in sight, even if they are able to surpass the U.S. and its allies on a technological level (Stone, 2020). Despite the damage to international relations this has caused, governments and businesses across the world still strive to have economic, and diplomatic ties with China.

Conclusion

China is currently the most dangerous cyber rival to the U.S., even if they aren't yet a direct rival. Their ability to couple sophisticated asymmetric cyberwarfare and information warfare with direct and indirect geopolitical pressure is not something we struggle to deal with. It has caused havoc among the Philippines, within Taiwan, and other key U.S. allies within China's sphere of influence. Even without launching cyber-attacks, it can be used to sway the public, and government of a nation for or against any asset China chooses to target. When actively utilizing cyber-attacks and information warfare, China utilizes proxies, offering them support while maintaining a plausible deniability should they be discovered and caught in the act. This makes it very difficult to pin the blame for cyberwarfare operations onto them, despite evidence seeming to support many cases. This also extends to cases of espionage against the U.S. and her allies where overwhelming evidence of Chinese operations have been discovered, but only limited reprisals, and consequences have been levied against them. Despite the U.S. operational, technological, economic, and political edge over China, they still seek to utilize their advantageous use of cyberwarfare to even the playing field, and find a loose parity with the U.S. I believe that overtime, if the U.S. cannot find a way to effectively combat Chinese cyberwarfare attempts, or limit their efforts, they will well and truly become a direct rival to the U.S. on the world stage.

References:

Campbell, L. M. (2023, June). *The Philippines: Cyber threats*. Defense Technical Information Center. https://apps.dtic.mil/sti/trecms/pdf/AD1213133.pdf

Canfil, Justin K., The illogic of plausible deniability: why proxy conflict in cyberspace may no longer pay, *Journal of Cybersecurity*, Volume 8, Issue 1, 2022, tyac007, https://doi.org/10.1093/cybsec/tyac007

Hannas, W. C., & Tatlow, D. K. (2021). *China's quest for foreign technology: Beyond espionage*. Routledge Taylor & Francis Group.

Hart, T. G. (1983). Sino-Soviet State Relations 1969-1982: An Attempt at Clarification. Cooperation and Conflict, 18(2), 79-99. https://doi.org/10.1177/001083678301800202 \

Jinghua, L. (2019, April 1). *What are China's cyber capabilities and intentions?* . Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

Kelter, F. (2022, November 9). *The battle over semiconductors is endangering Taiwan*. Foreign Policy. https://foreignpolicy.com/2022/11/09/tsmc-taiwan-battle-semiconductors-water-resource-scarcity/

Miller, M., & Gedeon, J. (2024, January 11). *Taiwan bombarded with cyberattacks ahead of election - politico*. Politico. https://www.politico.com/news/2024/01/11/taiwan-cyberattacks-election-china-00134841

O’Conner, S. (2019, May 6). *How Chinese Companies Facilitate Technology Transfer from the United States*. uscc.gov. https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf

Pacheco, O. Y., Yoachimik, O., Pacheco, J., & Tomé, J. (2024b, January 31). *DDoS threat report for 2023 Q4*. The Cloudflare Blog. https://blog.cloudflare.com/ddos-threat-report-2023-q4

Scissors, D. (2021, July 16). *The rising risk of China’s intellectual*-property *theft | American ...* American Enterprise Institute . https://www.aei.org/articles/the-rising-risk-of-chinas-intellectual-property-theft/

Standish, R. (2021, December 13). *How China became a force in the former Soviet space after the fall of the U.S.S.R.* RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/china-ussr-soviet-space-russia/31605573.html

Stone, J. (2020, October 5). *Foreign spies use front companies to disguise their hacking, borrowing an old camouflage tactic*. CyberScoop. https://cyberscoop.com/chinese-iranian-hackers-front-companies/

Swigart, Caleb John. *[China’s Influence in the Philippines]*. Maxwell Air Force Base, Alabama: [Air War College], 2023. Print.

Wiseman, G. (2015). *Isolate or engage: Adversarial states, US foreign policy, and public diplomacy*. Stanford Univ. Press.

Xu, M., & Lu, C. (2021). China–U.S. cyber-crisis management. *China International Strategy Review*, *3*(1), 97–114. https://doi.org/10.1007/s42533-021-00079-7