The PRC and the Cyber Pax Sinica: Growth in the Shadow of Pax Americana

Samuel Sheffield, 1LT, USAR, M.S. (Webster University)

Introduction

China has utilized every intelligence discipline at its disposal and has combined intelligence disciplines in creative, clandestine, and effective ways. As a result, presently the country's influence is rising rapidly and with a great deal of nuance and interconnectedness on a global level. Indeed, concern has been expressed that the People's Republic has *already* upset the stability of Pax Americana, bolstered by its cyberintelligence capabilities. This contribution serves as an overview of the methods used by the PRC to advance their goals, focusing on a) the ways in which history informs China's approach and b) the interconnected nature of Chinese foreign and domestic policies and the implication of this for the PRC's intelligence capabilities.

Definitions

Cyber intelligence has proved to be a difficult term to define, although some might think the term is fairly intuitive and includes anything computer or network related. However, there is more to cyber intelligence than just computers: at the most fundamental level, the umbrella term includes information taken or collected from any type of information source that has anything to do with some form of interconnected technology or media representation accessed through various technology suites. Complicating matters, an understanding of cyber intelligence must also account for the concepts of cyber threat and cyberspace. Here, we prioritize the Defense Counterintelligence and Security Agency's (DCSA) definition of a Cyber Threat: "Natural or man-made incidents (intentional or unintentional) that would be detrimental to the cyber domain,

or which are dependent on or operate through cyberspace/cyber domain."[1] Further, the United States Department of Defense (DoD) defines cyberspace as: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2]

Cyber intelligence has been especially difficult to define because it touches all five of the traditional intelligence collection disciplines: 1) Human Intelligence (HUMINT); 2) Signals Intelligence (SIGINT), which typically includes: COMINT (Communications Intelligence) and ELINT (Electronic Intelligence); 3) Geospatial Intelligence (GEOINT), most commonly involving Imagery Intelligence (IMINT); 4) Measurement and Signatures Intelligence (MASINT); and finally, 5) Open Source Intelligence (OSINT).[3]

China and Cyberintelligence: The Historical View

As noted by prominent scholars of modern China, the government of the PRC has consciously incorporated the study of history in the formulation of their policies, both domestic and foreign, drawing lessons from the experiences of other powers that may be usefully applied to the long-term project of ensuring Chinese dominance.[4] For example, it is at present an open secret that China understands its relationship with the United States in terms of strategic rivalry, a game that China fully intends to win, with a stated preference for "multipolarity" as only one way of expressing the intent to undermine U.S. global hegemony. Doing so means selectively

[1] DCSA, "Insider Threat Job Aid: A Glossary of Basic Insider Threat Definitions," 2017. cdse.edu. Ed. Defense Counterintelligence and Security Agency, https://www.cdse.edu/documents/cdse/CDSE-Insider-Threat-Definitions.pdf.
[2] C. A. Thehary, *Defense Primer: Cyberspace Operations* (Washington, DC: Congressional Research Service, 2018), https://fas.org/sgp/crs/natsec/IF10537.pdf.
[3] M. Chapple and D.Seidl, *Cyberwarfare: Information Operations in a Connected World* (Burlington, MA: Jones et Bartlett Learning, 2015).
[4] Cf. M. Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: St. Martin's Griffin, 2016).

borrowing from the toolbox that made the United States so successful, while eschewing those aspects of the American model that China understands as weaknesses. Most obviously, the Chinese early on understood the positive effects of economic liberalism in the United States and other western democracies (as well as Japan) and made corresponding adjustments in their economic investment strategies in the directions of "free competition" and a "self-regulating market"[5]; at the same time, the PRC has studiously avoided introducing political liberties, as these are understood as a threat to both the communist party's domestic dominance and to China's ambitions on the global stage.

When it comes to the PRC's approach toward cyberintelligence, as the Chinese regime has clearly drawn certain lessons from key junctures, namely, the outcome of the bipolar struggle between the United States and the USSR, as well as the factors that sustained the period of unprecedented American military and economic dominance after 1990. Specifically, in the late 1970s and early 1980s, the United States already began to enter the information age, where "informatization," or new computer-based communication techniques, were used to further develop the nation's economic and military abilities.[6] This, in combination with economic and manufacturing strength, gave the United States a decisive advantage over the USSR. Further, even more than contributing to the end of the Cold War, the rapidly developing new technologies seemed to solidify American dominance in its wake. Indeed, Pax Americana, in the Chinese understanding, would not have been possible without the introduction of (at the time) cutting-edge communication technologies.

[5] H. Cheung, "Is Putin Right? Is Liberalism Really Obsolete? June 28, 2019, https://www.bbc.com/news/world-europe-48798875.
[6] M. Porat, *The Information Economy*. Department of Communication, Stanford University, 1976

The immediate example of this was of course the outcome of the 1991 Gulf War. U.S. armies integrated technology on the battlefield in ways that overwhelmed and confounded the enemy due to a tenfold increase in U.S. communication and targeting abilities. According to Gady, "U.S. advanced military technology (e.g., precision-strike weapons) in particular is said to have destroyed Iraqi military hardware and broken the will of Iraqi soldiers to resist, negating the need to expose coalition soldiers to close combat." The consequences were felt far beyond Iraq, as "the astounding victory in the Gulf War was studied by militaries across the world. China especially saw the Gulf War as a wakeup call to modernize and reform the People's Liberation Army (PLA) through comprehensive digitization and networking in order to create a new joint force capable of fighting "Local Wars Under High-Technology Conditions."[7]

According to Lyu Jinghua, "Impressed by how the US military benefited from the application of high technologies in the Gulf War—and subsequent operations in Kosovo, Afghanistan, and Iraq—China began to realize that there is no way to adequately defend itself without following the changes in the forms of war in which high technologies, mainly information technologies, play more critical roles."[8] Thus, in 1993, two years after the Gulf War, the Chinese military adjusted its military strategic guideline, setting "winning local wars in conditions of modern technology, particularly high technology" as the basic aim of preparations for military struggle (PMS). Reflecting the growing importance of information technologies in the subsequent decade, in 2004, one year after the Iraq War, the Chinese PMS was changed to "winning local wars under conditions of informationization." The basic understanding, as elaborated in China's

[7] F. Gady, "What the Gulf War Teaches about the Future of War," *The Diplomat* March 2, 2018, https://thediplomat.com/2018/03/what-the-gulf-war-teaches-about-the-future-of-war/.
[8] L. Jinghua, "What Are China's Cyber Capabilities and Intentions?" Carnegie Endowment, April 1, 2019, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

National Defense doctrine in 2004, is that "informationization has become the key factor in enhancing the warfighting capability of the armed forces."[9]

Furthermore, when it comes to cyber warfare specifically, the PRC's perception is that it permeates through all aspects of life, leadership, and statecraft. Chinese military analysts often define cyber warfare as "strategic warfare in the information age, just as it was nuclear warfare in the twentieth century. This definition serves as the foundation to argue that cyber warfare has much broader significance to national security and involves competition in areas beyond the military, such as the economy, diplomacy, and social development."[10]

This definition of cyber warfare is reflected in the PRC's establishment of the Strategic Support Force (SSF), which is the counterpart of the United States' Cyber Command. However, the SSF's scope is far more expansive than that of similar structures in other countries in terms of command and control of intelligence assets: "[The SSF] uniquely conducts several different missions simultaneously that in the U.S. would be happening at the National Security Agency, Army, Air Force, Department of Homeland Security, NASA, State Department and Cyber Command, among others. If you combined all those government entities and added companies like Intel, Boeing, and Google to the mix, then you would come close to how the SSF is built to operate."[11]

On the one hand, China's integration of all things related to cyber intelligence under one roof reflects the modus operandi of modern Chinese military intelligence operations, an approach that has, historically, had certain limitations. Throughout the second half of the twentieth century, in fact, China was (disparagingly) known for choosing quantity over quality in this sense:

[9] Ibid.
[10] Ibid.
[11] C. Bing, "How China's Cyber Command is Being Built to Supersede Its U.S. Military Counterpart," June 22, 2017, *CyberScoop*, https://www.cyberscoop.com/china-ssf-cyber-command-strategic-support-force-pla-nsa-dod/.

> If a beach was an espionage target, the Russians would send in a sub, frogmen would steal ashore in the dark of night and with great secrecy collect several buckets of sand and take them back to Moscow. The Americans would target the beach with satellites and produce reams of data. The Chinese would send in a thousand tourists, each assigned to collect a single grain of sand. When they returned, they would be asked to shake out their towels. And they would end up knowing more about the sand than anyone else.[12]

This dismissive approach toward Chinese intelligence gathering methods notwithstanding, it is true that China has favored nonstandard intelligence sources, with their methods becoming much more sophisticated as their technology has improved. China has developed its military and cyber capabilities based on the trial and error of other countries, mainly the U.S. and Russia, while at the same time preferring to use an indirect approach to expand their reach. Chinese cyber intelligence actors, along with other intelligence disciplines, rely on methods that may not seem like they are tied to gathering intelligence or directing events; often, these include conducting silent information warfare by utilizing ties to domestic and foreign economic and entertainment industries.

When it comes to cyber intelligence gathering in economics and business, PRC intelligence agencies utilize any means and information sources available to them. Private companies (Chinese and foreign) are compelled to adhere to the communist government mandate if they want to operate within Chinese borders,[13] meaning that any type of technological advancement is ultimately under the aegis of the Communist Part of China (CPC), as businesses wishing to operate within Chinese borders must agree to cede over control and/or oversight of their business assets located in the country. There has been an abundance of complaints about foreign businesses being forced to share technology, business, and trade secrets with the Chinese

[12] P. Mattis, "A Guide to Chinese Intelligence Operations," *War on the Rocks* August 18, 2015, https://warontherocks.com/2015/08/a-guide-to-chinese-intelligence-operations/.
[13] Bing, "Chinese Cyber Command."

government in order to gain access to the burgeoning Chinese economy. Officially, this forced technology transfer is expressly forbidden in Chinese law; the government itself consistently denies that it is happening: "Beijing thinks all the accusations of forced technology transfer and IP [Intellectual property] theft are groundless … The discrepancy is huge and there is no common understanding on the IPR issue; China can and will do nothing to address the problems that do not exist."[14] This obfuscated denial, typical of Chinese officials, belies the fact that China requires foreign companies to conduct joint ventures with a Chinese representative or business in order to do business within Chinese borders.

These joint ventures usually entail giving 50 percent of the ownership to the Chinese representative, along with giving rights to certain or all aspects of whatever product the company is attempting to sell or manufacture in China. These joint ventures end up circumventing Chinese law that expressly bans forced intellectual property transfer because the PRC does not "discriminate" between stated owned and private companies, meaning that they receive equal attention and are treated similarly.[15] As a result, Chinese-owned private enterprises (including joint ventures with foreign companies) are beholden to give up control and possibly intellectual property rights upon governmental request.

There have been many examples where a foreign company sets up a joint venture to share risk and gives partial ownership to their Chinese counterparts, who then takes the assets from the foreign company with the promise of shared profits:

[14] J. Cai, "Trade War: Why US and China Remain So Far Apart on IP Rights," October 8, 2018, https://www.scmp.com/news/china/diplomacy/article/2166315/trade-war-why-us-and-china-remain-so-far-apart-intellectual.

[15] C. Zhou, (2019, March 18). "China Will Not 'Discriminate' between State and Private Companies," March 18, 2019, https://www.scmp.com/economy/china-economy/article/3001921/china-will-not-discriminate-between-state-and-private.

> The Chinese company will then either go silent or—if it still needs the foreign company—it will provide it with *fake* documents showing the joint venture was in fact formed with the foreign company having ownership in it. The foreign company believes it owns part of the China joint venture even though it does not. Eventually (usually many years later) the foreign company starts getting frustrated about never receiving any money or even news from the joint venture and contacts a China lawyer for help…. The bad news is that there is usually nothing that can economically be done to help a foreign company in this sort of situation.[16]

While this indirect coercion is one manifestation of Chinese intelligence practices using nonstandard intelligence operators to gather information and/or influence outside actors, it coexists with other, more conventional forms. Crucially in the latter respect, China has continued to extend the reach of the Publicity Department of the Communist Part of China by cultivating a positive image in world media.

The Publicity Department (PD) was created by Mao Zedong during the second Sino-Japanese War (1937–1945), at which time Mao instituted a policy of placing journalism after politics, known as "Maoist Journalism." The PD was meant to educate the Chinese people on the beliefs and stances of the CPC, and to also control, monitor, and censor opinions, publications, and various art/media forms.[17] Today, the Publicity Department controls four important aspects of Chinese public culture:

1) Ideology – The Theory and Education Bureaus are in charge of maintaining and managing CPC policies and theories.

2) Culture and Arts – The PD encompasses the Ministry of Culture and the State Administration of Press, Publications, Radio, Film and Television (SAPPRFT), which deals with CPC representation within Chinese media.

[16] D. Harris, "China Joint Ventures: The Long Version," February 3, 2019, https://www.chinalawblog.com/2019/02/china-joint-ventures-the-long-version.html.
[17] J. Wu, "A Look Inside China's Propaganda Bureaucracy," November 12, 2017, https://advox.globalvoices.org/2017/11/12/a-look-inside-chinas-propaganda-bureaucracy/.

3) Education and Research – the PD works to ensure that CPC indoctrination is introduced at every level of education and social science/philosophical research.

4) International Publicity – The PD has an International Communication Office that conducts business and interchanges with foreign media and is in charge of curating a positive international Chinese image while informing the world on Chinese policies and news.[18]

The PD has also invested in media and entertainment companies around the world, and the increased demand for western-style movies and TV shows has caused many Hollywood types to expand into the Chinese market. Again, in order to do business in China, there are some prerequisites: "China has become a hugely lucrative market for American films—causing pushback from some in the ruling Chinese Communist Party, who fear the spread of ideas they find distasteful. And so Hollywood producers work with Beijing to ensure that their scripts won't, in Chinese parlance, 'hurt the feelings of the Chinese people.'"[19] Hollywood producers and those in the entertainment industry see no issue with censoring themselves or making "corrections" in order to appease a country, of which, most of their consumers hold in a positive view: As of 2018, a majority (53 percent) of Americans have a positive view of China.[20]

Expanding China's influence via positive image making abroad has been enabled by the country's further development of its communication networks and modernization efforts from acquired technology:

> Premier Li Keqiang's 2015 Government Work Report inaugurated a new term for information technology policy: "Internet Plus." This initiative, which aims to "integrate mobile Internet, big data, cloud computing and the Internet of Things," is the latest iteration of a broader strategy to build China into a "strong Internet power" … New, high-

[18] Ibid.
[19] I. S. Fish. (2018, March 30). "The Coming Chinese Crackdown on Hollywood," March 30, 2018, https://www.washingtonpost.com/news/democracy-post/wp/2018/03/30/the-coming-chinese-crackdown-on-hollywood/?utm_term=.06a79a852f82.
[20] Gallup, Inc. "Favorable Views of Japan, China Keep Climbing," March 6, 2018, https://news.gallup.com/poll/228638/favorable-views-japan-china-keep-climbing.aspx.

> level regulatory institutions were established which promulgated new rules on subjects ranging from malicious software on mobile app stores to the use of social media accounts. These changes… demonstrate an intention to place technology at the centre of an ambitious agenda for comprehensive reform of social and economic governance.[21]

These policy changes instituted in 2015 have led to a further governmental access to a mass of information that can be channeled into cyber intelligence products.

The PRC's foray into additional population monitoring and influencing, along with micromanaging their global image, indicates a deeper intention of obvious and direct expansion of their influence. In 2018, U.S. Director of National Intelligence Dan Coats stated that the Chinese have become increasingly aggressive in their intelligence gathering, while still retaining their methodical pace. In his view, Chinese advancing technical proficiency is a bigger threat than Russia's attempts to influence the 2016 U.S. elections; at the same time, "China's slow and careful operations [has] helped the government escape the kind of publicity that has followed Russia's actions."[22]

The expansion of Chinese cyber intelligence capabilities and soft-power influence has occurred simultaneously, if not despite, developments related to this sphere in the official realm of U.S.-China relations. Thus, in September 2015, the United States and the People's Republic of China signed a cyber security agreement, stating that both countries would not conduct intellectual property theft or steal commercial trade secrets and would not enable or encourage anyone else to do so. The agreement did not cover government to government spying but instead

[21] R. Creemers, "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century," September 5, 2016, https://www.tandfonline.com/doi/full/10.1080/10670564.2016.1206281.
[22] Voice of America, "US Intelligence Chief Warns of China's Improved Cyber Spying," October 3, 2018, https://learningenglish.voanews.com/a/us-intelligence-chief-warns-of-china-s-improved-cyber-spying/4591156.html.

was supposed to establish an ongoing dialogue between the two governments to be used to request investigations into commercial hacking attempts or incidents.[23]

Perhaps as a result of this agreement, Chinese-initiated cyberattacks against the United States dropped significantly in 2015 and 2016; however, they slowly began to rise in 2017, but with increased sophistication. In contrast to the smaller or individualized attacks that had characterized Chinese behavior previously, the attacks focused more on aggregated data and cloud repositories. In part, researchers have understood as a response to increased anti-Chinese rhetoric from U.S. President Trump, though it must be pointed out that by September 2018 they had again shown decreasing trends, indicating the link may not be as strong as initially suspected (the decrease in frequency of attacks, on the other hand, could be interpreted as indicating a rise in their operational efficiency).[24]

Crucially, Chinese cyberattacks against American targets since 2015 are characterized by their use of system ready tools alongside software made specifically for a particular attack and then remain undetected for days or months (possibly longer) before the intrusions are found:

> [They used] multiple command and control (C&C) systems to communicate with backdoors and other malware, with at least one of them on a "sleep cycle"—left inactive until after other C&C systems have been purged by the targeted organization's security team. [They also have used] "Living off the land" [or] moving within the targeted network by using "known good tools" (legitimate software packages or system tools that may already be installed on the target network). [Additionally, they have used] techniques such as process hollowing to conceal malicious code within an existing system process to evade detection, Windows Management Instrumentation, and other alternatives to [legitimate software packages or tools] to conceal activity on Windows systems.[25]

[23] B. Acohido, "What You Need to Know about the China-U.S. Cyber Security Pact," October 13, 2015, https://cyberscout.com/education/blog/what-you-need-to-know-about-the-china-us-cyber-security-pact.
[24] R. Abel, "Decline in Chinese Cyberattacks against U.S. Suggests Attacks Getting More Efficient," September 28, 2018, https://www.scmagazine.com/home/security-news/decline-in-chinese-cyberattacks-against-u-s-suggests-attacks-getting-more-efficient/.
[25] S. Gallagher, "New Data Shows China Has 'Taken the Gloves Off' in Hacking Attacks on US," November 1, 2018, https://arstechnica.com/information-technology/2018/11/new-data-shows-china-has-taken-the-gloves-off-in-hacking-attacks-on-us/.

These attack methods fall in line with the PRC's published Military Strategy, which includes

> cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace, and participation in international cyber cooperation… [with aims of] stemming major cyber crises, ensuring national network and information security, and maintaining national security and social stability.[26]

Perhaps most importantly, in the Chinese case it should be understood that the PRC sees an unbreakable link between social stability and national security, which is in turn strengthened by China's growing influence outside its borders; in this age of rapidly changing technology, cyber (and other forms of) intelligence becomes crucial for maintaining all three sides of this equation. Tight control over the population domestically, enhanced by information technologies, makes it easier for the Chinese state to focus on its role on the international stage. According to Human Rights Watch,

> [In 2018] Human rights defenders continue to endure arbitrary detention, imprisonment, and enforced disappearance. The government maintains tight control over the internet, mass media, and academia. Authorities stepped up their persecution of religious communities, including prohibitions on Islam in Xinjiang, suppression of Christians in Henan province, and increasing scrutiny of Hui Muslims in Ningxia.[27]

Conclusion

As strains in the relationship between the United States and China continue to gather steam, especially in the context of the Covid-19 viral pandemic and the questions surrounding both its origins in Wuhan and the Chinese government's employment of methods discussed in this article to spread misinformation aimed at whitewashing the extent to which the PRC has mismanaged the

[26] Jinghua, "What Are China's Cyber Capabilities and Intentions?"
[27] Human Rights Watch, "World Report 2019: Rights Trends in China," January 17, 2019, https://www.hrw.org/world-report/2019/country-chapters/china-and-tibet.

crisis, it becomes more vital than ever to understand Chinese intelligence capabilities. This article has argued that the Chinese approach is driven by three factors. First, the important role assigned to history by the Chinese regime means that it learned vital lessons about the value of information and other high technologies in the ultimate victory of the United States over the Soviet Union, lessons that have led it to invest heavily in information technology and cyber intelligence capabilities in the service of its own rivalry with the United States. Second, capitalism in China remains heavily state-driven, meaning that the government can utilize its 50 percent stake in companies doing business in China for intelligence gathering purposes. Finally, there exists a feedback loop between the Chinese regimes use of communication technologies to disseminate pro-Chinese propaganda and misinformation abroad (as part of its effort to raise the PRC's global influence) and the use of the same kinds of technologies to a) shore up regime via propaganda and education campaigns at home and b) employ cyber technologies to monitor the Chinese population and suppress dissent. As the world enters the unknown waters of a globe ripped apart by the Covid-19 epidemic, ensuring the continuing leadership of the United States requires full comprehension and awareness of the scale and direction of Chinese use of cyber-related technologies as the PRC regime consciously pursues a path toward disrupting and ultimately displacing American hegemony.