The Strategic Outset: China’s Cyber Campaign to Initiate an Invasion of Taiwan

Capt David M. Moore

Squadron Officer School

Class 21D, Flight C-44

21 May, 2021

"Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air University, the United States Air Force, theDepartment of Defense, or any other US government agency."

Abstract

Based on Chinese doctrine, demonstrated capabilities, and strategy, the PRC will likely leverage existing influence in public sector technology and the open internet to execute large scale cyber-attacks scoped to the South Pacific at the outset of conflict with Taiwan. The PRC intends to isolate the battlespace while disrupting C2 and logistics in order to swiftly achieve their strategic objective, discourage third party intervention, and minimize the likelihood of war with the United States. A consideration of low-tech communication solutions and historic C2 methods may be key for the U.S. to mitigate the "fog of war" created across the battlespace, mount an effective response in support of Taiwan, and control the risk of miscalculated actions to avoid unintended escalation.

Main Body

Doctrine

The first step in outlining China's phase 0 strategy is to identify key trends in their doctrine and presumed intent. In most cases, Chinese operators do not care if they get caught in the act of conducting cyber infiltration. China boasts the ability to demonstrate such capabilities as a form of deterrence. Viewed in similar light to nuclear deterrence, by demonstrating these capabilities, they hope to use the mere known existence of cyber techniques and weapons as a means to deter provocative behavior from their adversaries.[1] The drastic difference between cyber and nuclear warfare, however, is in the realm of international law and treaty. Because so much of cyberspace is a military grey area, there are no standards in place to govern action taken across this domain. Major powers hesitate signing laws or treaties to regulate cyber activity as well, since each country knows that weapons and techniques in cyberspace are internally derived and give an upper-hand such that without demonstrating the weapon no effective defense may be developed.[2] This drives a need for cyber weapons to be used as first strike options, to field the weapon and achieve desired effects before a defense or justified retaliation may be mounted. Additionally, a state may perceive cyber attacks as more serious or damaging than the attacking state intended. So China must balance the risk of unmatched retaliation against the benefits of first strike actions likely to occur.

As China continues to position itself as a global power, support and influence of the international community remains a paramount concern. China will likely frame any military action taken

[1] Lora Saalman, "Pouring 'New' Wine into New Bottles: China-U.S. Deterrence Relations in Cyberspace," *Seton Hall Journal of Diplomacy and International Relations*, (2015/2016 Special Issue): 25.
[2] Julija Kalpokiene, Ignas Kalpokas, "Contemplating a Cyber Weapons Convention: An Exploration of Good Practice and Necessary Preconditions," *Baltic Journal of Law & Politics* 13, no. 1 (2020): 56.

against a sovereign state as either retaliatory or in the case of Taiwan as a matter internal to the Chinese nation. Because of this, China will focus their cyber strategy around maintaining their international reputation and indirectly making third party intervention as difficult and risky as possible. U.S. force posturing is their biggest obstacle to this objective. One foreboding similarity between the United States' and China's military doctrines are their forward-deployment-oriented force dispositions. China will forward position troops, equipment, and capabilities when they perceive a change in adversary position or intent, in order to maintain the upper hand and be preemptively prepared for action when necessary (known as China's Active Defense doctrine).[3] With opposing forces spread throughout the region and "fog of war" across the battlefield, the risk of incidental escalation becomes dangerous.[4] Additionally, China's stance toward state-on-state aggression is clear- they will avoid conflict when possible but will surely counterattack if attacked.[5] This provides the opportunity to maintain deniability and save face within the international community, thus holding leverage to discourage U.S. involvement.

Demonstrated Capabilities

With doctrine outlined, this next section highlights demonstrated capabilities in the public sector and open internet that China will likely leverage in a campaign against Taiwan. There are good cost incentives for technology companies to outsource operations to China. Such programs were intentional on part of the Chinese government. Most Chinese technology and telecommunication firms are contracted by and tied into the government's infrastructure.[6] Additionally, in 2003 China purchased the rights from Microsoft to study their Windows OS source code as a

[3] Muhamad Ali Baig, "Conventional Military Doctrines and U.S.-China Military Engagement in the West Pacific." *China Quarterly of International Strategic Studies* 5, no. 3 (2019): 378.
[4] Ibid., 387.
[5] Ibid., 378.
[6] Ibid., 19.

contingency for doing business in their country, permitting the analysis of proprietary information fundamental to most Commercial-Off-The-Shelf (COTS) computers.[7] These two factors give China the platform to attack seemingly any system or network it wants at any time. Such actions were demonstrated in 2015 when China launched a cyber campaign against the Philippines, targeting their government, telecommunications, and energy sector systems. In line with their doctrine, China described these attacks as retaliation to aggression toward China in the South China Sea.[8] China's utilization of asymmetric cyber capabilities to pursue strategic objectives is further exemplified through operations across the open internet.

Similar to the lack of international laws governing use of cyber weapons, there are few international standards to dictate corporate protection of information, access, and systems through which their products and services operate.[9] As such, there is little to deter aggression against these companies to affect targeted populations. From 2017 through 2019 China utilized hundreds of fake Twitter accounts to target political opponents of the Chinese Communist Party. Such actions were observed on Facebook as well, and it is likely China maintains the ability to infiltrate these public forums in ways that remain undetected. 2019 also saw China carry out a massive Denial of Service (DoS) attack against Telegram, the message app used to organize protests in Hong Kong. This shut off access to more than 200 million users worldwide.[10] In 2020, China targeted Taiwan's presidential election. In the months leading up to the election,

[7] Jayson Spade, "China's Cyber Power and America's National Security," (master's thesis, Army War College, 2011), 25-27.

[8] Mark Bryan Manantan, "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea," *Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs* 56, no. 3 2040013 (2020): 16.

[9] Karen A. Scarfone, Daniel R. Benigni, Timothy Grance, "Cyber Security Standards," in *Wiley Handbook of Science and Technology for Homeland Security* (Hoboken: John Wiley & Sons, Inc., 2009), https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153: 2.

[10] Ibid., 12.

Taiwan's national infrastructure suffered between 10 and 40 million attacks per month. These attacks spread fake news and disinformation about the candidates and Taiwan's security. They altered information Taiwanese citizens would see online, and bombarded users with malicious information to the extent that internet services were degraded nationwide; China openly claimed responsibility.[11]

Strategy

By tying China's stated doctrine and demonstrated intent into the tools and tactics observed in the cases above, we can outline China's likely strategy at the outset of a conflict with Taiwan, broken into three lines of effort. First, China will carry out unparalleled messaging campaigns across the open internet to identify Taiwan as the initial aggressor. The accusations will likely center around malicious cyber actions, as rapid confirmation by outside sources would be difficult. Based on China's denial of Taiwanese independence, messaging will identify the conflict as an internal matter to be handled swiftly. As such, China will likely state that third party intervention is unwelcome and will be met with force. A simultaneous communication blackout of Taiwan is expected, to control the narrative and isolate the enemy's Command, Control (C2), and logistics. Next, China will deny network and communications access throughout the South Pacific. Finally, China will cut GPS access throughout the region, forcing assets of all parties to navigate and maintain battlespace awareness by other means, a scenario some would argue that is well rehearsed by Chinese forces.[12] These calculated actions create

[11] Ibid., 10.

[12], James Palmer, "China Intensifies Provocations Over Taiwan," *Foreign Policy*, 14 April 2021, https://foreignpolicy.com/2021/04/14/taiwan-china-jets-incursions-military-tensions/.

battlefield conditions intended to deter third party intervention from players, such as the United States.

It is very unlikely that China will take direct action against the United States and military allies, other than Taiwan, during this phase of operation. China must save face to the international community, putting the move toward state-on-state conflict on such third parties. Communication and GPS blackouts will affect all parties operating in the South Pacific equally. China's invasion across other domains will likely begin within moments of these actions, and through overwhelming force, may achieve operational objectives before a response is mounted. Immediately, U.S. and allied forces in the region will assume a heightened state of alert fueled by the "fog of war" of an isolated battlespace and lack of unified direction. U.S. defense officials believe the best chance of success in this scenario will depend on the ability to operate in spite of these limitations.[13] Although due to U.S. strategic understanding of this situation, a response would either be intentionally scaled back until C2 and mass coordination is worked out or miscalculated, incidentally triggering Chinese response and undesired armed conflict. From China's perspective, strategic objectives must be met before any response is mounted. Otherwise, they gamble on the United States' willingness to support Taiwan at the risk of peer conflict. China must decide the timing is right to initiate invasion by balancing its necessary international reputation with the current state of affairs in Taiwan, and the posture of opposing forces.

[13] Robert Work, interview by Strategic Studies Quarterly, *China's Competitive Strategy: An Interview with Robert. O. Work*, Strategic Studies Quarterly, Spring 2019, 3.

Conclusion

By piecing together China’s doctrine and demonstrated capabilities, a baseline of what to expect from China’s initial cyber strategy at the outset of war with Taiwan may be gleaned. The limitations to this paper revolve around the unclassified nature of research conducted, so additional capabilities will likely be fielded to bolster their intended effects on the battlespace. U.S. forces must develop courses of action to operate in such an isolated environment in order to uphold our commitments while avoiding unintentional escalations of force. As with China’s strategy, our continued operations do not necessarily require high tech solutions. Innovation and strategic design problem solving for this scenario should not just focus on throwing the most money at development of more advanced technologies. Outside the box approaches and level thinking will lead us to the proper courses of action to prevail through distributed control and decentralized execution on the battlefield. A lot may be gained by looking back at the Berlin Airlift; while the enemy's capabilities are far more advanced today, our C2 and logistics abilities could very well be limited back to what they were in the 1940s. An example innovation is investment in low-tech or “analog” connections with Taiwan that remain separated from communication networks, such as running isolated cables to the island. If we consider the low-tech approach, the U.S. would be able to maintain communication once China’s strategy is initiated, and coordinate support when the island is under complete siege soon after. The U.S. will doubtfully best China in this outset scenario, especially if conflict were to happen in the next 5 years as some suggest. Thus, we should go back to the basics and get creative so that we can carry out an effective response while minimizing the risk of a war many are not sure we can win. While victory would require a joint all-domain approach, there is no doubt this fight will begin in cyberspace.

References

Ammerlahn, Heidi, Farr, Scott,McClane, William, Pavelko, Robert. “Dancing with the dragon: U.S. cyber engagement with China and the Asia-Pacific region.” Harvard University, 2012.

Baig, Muhamad Ali. “Conventional Military Doctrines and U.S.-China Military Engagement in the West Pacific.” *China Quarterly of International Strategic Studies* 5, no. 3 (2019): 373-393.

Clarke, Richard A. “The Risk of Cyber War and Cyber Terrorism.” *Journal of International Affairs* 70, no. 1 (Winter 2016): 179-181.

Johnson, James S. “Chinas vision of the future network-centric battlefield: Cyber, space and electromagnetic asymmetric challenges to the United States.” *Comparative Strategy* 37, no. 5 (2019): 373-390.

Kalpokiene, Julija, Kalpokas, Ignas. “Contemplating a Cyber Weapons Convention: An Exploration of Good Practice and Necessary Preconditions.” *Baltic Journal of Law & Politics* 13, no. 1 (2020): 51-80.

Manantan, Mark Bryan. “The People’s Republic of China’s Cyber Coercion: Taiwan, Hong Kond, and the South China Sea.” *Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs* 56, no. 3, 2040013 (2020): 1-29.

Palmer, James. “China Intensifies Provocations Over Taiwan.” *Foreign Policy*, 14 April 2021, https://foreignpolicy.com/2021/04/14/taiwan-china-jets-incursions-military-tensions/.

Saalman, Lora. “Pouring ‘New’ Wine into New Bottles: China-U.S. Deterrence Relations in Cyberspace.” *Seton Hall Journal of Diplomacy and International Relations*, (2015/2016 Special Issue): 23-35.

Scarfone, Karen A., Benigni, Daniel R., Grance, Timothy. “Cyber Security Standards” in *Wiley Handbook of Science and Technology for Homeland Security*. Hoboken: John Wiley & Sons, Inc., 2009. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153.

Spade, Jayson. “China's Cyber Power and America's National Security.” Master’s thesis, Army War College, 2011.

Work, Robert. Strategic Studies Quarterly. “China’s Competitive Strategy: An Interview with Robert. O. Work,” *Strategic Studies Quarterly*, Spring 2019.