Cyber Deterrence: Controlling Escalation in Taiwan

Capt Allison R. Ramos

Squadron Officer School

Class 21-D, Flight B-19

Abstract

Over the past year, there have been growing tensions between China and Taiwan, and evidence points to a situation where China could take over the country within a few years. The US has pledged to defend Taiwan through national-level guidance. To do so, it must work with allies in the area such as Australia, Japan, The Republic of Korea, and the Philippines to create and execute an active denial-based cyber deterrence strategy. For the US to be successful, the strategy will have three parts. The first part is the forward deployment of US cyber personnel to the countries mentioned above and their cyber centers while broadcasting the movements through the media. The second is drawing red lines in cyberspace to alert China of what is or is not acceptable. Finally, the third part is the response. The US will develop preapproved actions to decrease response time to Chinese cyber aggressions if they cross any red lines. Without forward-deployed cyber personnel, Taiwan will be unable to secure cyberspace.

The United States (US) should forward deploy a cyber presence to multiple countries in the Indo-Pacific area of responsibility, showing America resolve and an international alliance to deter actions against Taiwan.

Background

Admiral Davidson, Commander of US Indo-Pacific Command (USINDOPACOM), stated before the Senate Armed Services Committee that China views Taiwan as its number one priority, and research indicates that they could take the country within six years.[1] As such, Taiwan has gained much of the international community's attention. However, only 15 countries recognize Taiwan as a singular country and not part of China as part of the "One China Principle".[2] The US is a primary supporter of Taiwan and explicitly includes them to defend in National Security Strategies throughout the years . Other countries, and US allies, that are physically in the best positions to help Taiwan from an invasion scenario are Japan, the Republic of Korea (ROK), the Philippines, and Australia.[3] However, many countries are hesitant about standing up to China for various reasons. The ROK is concerned that supporting Taiwan would lead to military conflict with North Korea, potentially harming the mass amount of military troops on the peninsula.[4] While Philippine President Duterte pledged his allegiance to China in 2016, it's clear that he disagrees with China's actions in the South China Sea and threats to the Philippine's land and sea territories.[5] Duterte is left with few options except foreign relations, especially with the US, to deter China.[6] Australia has made relatively few comments on the situation but stated they would maintain current policies towards Taiwan.[7] Although, the statement lacks clarity on types of attacks or conditions that could arise in a conflict or any response actions from Australia.

Japan supports the defense of Taiwan from China. If China could control all trade through the area, Japan would be at its mercy for economic and national security.[8] While Japan has made no official comment on what they would do if China invaded Taiwan, it can be assumed that if China directly attacked any Japanese bases in a scenario, the US would align with Japan and support Taiwan.[9] The US has that they will defend Taiwan but has been vague about how that would happen.[10] The US canceled the Taiwan Relationship Agreement in 1979 and hasn't completed a large-scale military exercise together since that time.[11] While the US does send attaches and diplomats, they rarely stay long enough to build relations which could be a hindrance if the countries were presented with a multinational working environment.[12]

Assumptions

There are three assumptions for this discourse. First, the Chinese mainland will be harder to attack than any outstations by target selection and risk of escalation. Second, Chinese economic and diplomatic outposts, such as merchant fishers or mines, embassies, or ports in other countries, are legitimate response targets. Finally, the third assumption is that the Chinese abuse of international norms requires a more robust global response. If the rest of the world imposes costs on Chinese cyber aggression, China has multiple deterrent effects countering Chinese expansion.

Cyber Deterrence

The Deterrence Operations Joint Operation Guide (DOJOC) defines deterrence as the ability to "Convince adversaries to not take action that threaten US vital interests by means of decisive influence over their decision making … [to] change the decision calculus of an adversary by denying benefits, imposing costs, or encouraging adversary restraint."[13] One method to deter is the cyber domain is through a forward-deployed presence. The US Cyber

Command (USCYBERCOM) has included the concept as a central focus through superiority through persistence.[14] The goal is to deploy as close to the adversary activity as possible, allowing the research of weaknesses, intentions, capabilities, and ability to counter-attack.[15] USINDPACOM reinforces a cyber alliance with the ROK, Japan, and Australia to include information sharing and cyber attack response commitments.[16] It lists the Philippines as a nation that the US will support specifically in an armed attack in the South China Sea.[17] However, it does not mention Taiwan or cyber attacks. Forward deploying in cyberspace assumes that the US can act in cyberspace while controlling escalation and the persistence will deter others from cyber attacks.

Forward deployed troops allow for the normalization of cyber operations, which decreases the risk of escalatory response in a conflict situation. The decision to forward deploy in cyberspace includes cyber protection teams, operations within allied networks, operations against adversary networks, intelligence sharing with allies and partners, and using malware to set up critical national infrastructure to be effected.

The US must forward deploy troops because of the organizational decision to support Taiwan. The 2017 National Security Strategy included Taiwan and stated the US would provide for Taiwan's legitimate defense needs and help deter coercion.[18] The Interim National Security Strategy Guidance reaffirmed that guarantee, including comments that Taiwan is a democracy and critical economic and security partner in line with American commitments.[19] The US values democracy, human rights, and human dignity as the basis for all top-level doctrine and strategies. Each document includes spreading and securing democracy as part of its core mission. In a cyber event with China, China could stifle the fundamental right to freedom of information or speech through a DDoS attack as was seen in Hong Kong or a zero-day attack that could have strategic-

level effects on critical national infrastructure. The US must deter Chinese aggression towards Taiwan as aligned with their diplomatic pledge.

Recommendations

The US must develop a cyber strategy towards China and Taiwan that (a) develops a forward presence, (b) develops red lines in a cyber conflict that China cannot cross without consequence, and (c) if the lines above are crossed, the US and partners must hold China's national interests at risk through previously approved actions. The forward presence will be established by including a cyber center liaison officer to work with allies' cyber command centers. Australia's offensive and defensive cyber capabilities reside within the Australian Signals Directorate. According to the most recent Annual Report, they have been conducting offensive defense of the countries national interest.[20] Japan's cyber capabilities reside in the Ministry of Defense and maintain a response only posture towards cyberspace capabilities.[21] The increased US presence, through permanent positions or travelling delegations will allow members to become embedded in the systems remotely or physically through agreements or norms. The US has successfully integrated cyber officers in personnel exchange programs in the United Kingdom and Canada.[22] The US and ROK cyber agreement includes information sharing including critical national infrastructure, cyber event investigations, cybersecurity collaboration, and cybersecurity framework elements.[23] Additionally, the US has forward deployed cyber troops to Montenegro, Estonia, North Macedonia, and Ukraine to help protect the countries from within the foreign networks.[24] Finally, to make the world aware of the new posturing, information must be released to include relationship building and after-action reports of what was accomplished. It will also secure the information environment for the US aligning with multiple DOD guidance and increase the US's global credibility.

The second item, red lines, must be developed to know when a military response measure should be employed. In Hong Kong, Telegram, an encrypted messaging application, suffered a distributed denial-of-service (DDoS) attack to stop protestors from communicating.[25] When Telegram ceased to work, protestors moved to another messaging service that was vulnerable to attacks.[26] The change in situation allowed China the information advantage. While doctrinally, the US should not respond to human security violations, the argument could be made that if the military also used Telegram for recalls, it would give the US the green light required to respond to China's national interests. The same could be agreed on for other information systems that affect both the military and civilians. Additionally, social media hacking tools have been sold to governments to spy on citizens.[27] If China were found to use these tools to spy on military leaders or infiltrate a command and control epicenter, those would be red lines requiring a response from the US and partners.

Finally, if red lines are crossed, the US and allies must hold China’s interests at risk. One issue that arises with this is the authority to act in cyberspace. Per Joint Publication 3-12, Cyberspace Operations, the Commander USCYBERCOM, and the subordinate cyber commanders are the authority for offensive and defense cyber within the DODIN and other networks worldwide from a military perspective.[28] There is no guidance on if the control can be delegated down to a lower level. Creating specific pre-approved actions as actions that can happen quickly after a red line is drawn would remove doubt and empower the forward-deployed cyber troops to make near-real-time decisions. Including partners in the overall plan allows less tech-savvy allies to assist and could bring additional capabilities to complement US capabilities while meeting the intent of all top-level US strategic documentation.[29] China’s national interest in protecting national sovereignty, territorial integrity, and continued development of the

economy.[30] The fact that China wants the lead, both territorial and economically, in the AOR is echoed in the USINDOPACOM's strategy as one of the global defining elements of the 21st century.[31] The country continues to seek "regional hegemony in the near-term and ultimately global preeminence in the long-term."[32] Targeting maritime ports within the South China Sea including, but not limited to the Spratly, Paracel, and Senkaku islands, would allow the US a national interest target that would not be as protected as the mainland. Using interconnectedness as a deterrence element and strategic advantage, being forward deployed in the region would allow easy access to these Chinese national interest targets as well as posturing for a swift and immediate, proportional attack. If China violates the red lines and the US does not respond, it will be detrimental to the US's credibility.

In conclusion, the US must forward deploy cyber troops to the region to increase cyberspace deterrence to defend and protect Taiwan. Red lines must be declared, and pre-approved actions must be approved to empower the deployers to carry out the US strategic responses swiftly and proportionally. Only then will China's decision calculus be altered to not engage Taiwan in cyber conflict.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

[1] Shelbourne, "Davidson."

[2] Brimelow, "Fears of a Chinese Attack on Taiwan Are Growing."
[3] Ibid.
[4] Ibid.
[5] Grossman, "China Has Lost the Philippines Despite Duterte's Best Efforts."
[6] Ibid.
[7] Zheng, "Australia Will Maintain Its Taiwan Policy."
[8] Brimelow, "Fears of a Chinese Attack on Taiwan Are Growing."
[9] Ibid.
[10] White House, "Interim National Security Strategic Guidance."
[11] Brimelow, "Fears of a Chinese Attack on Taiwan Are Growing."
[12] Ibid.
[13] Department of Defense (DOD), "DOJOC."

[14] United States Cyber Command (USCYBERCOM) “Command Vision for USCYBERCOM.”
[15] Ibid.
[16] DOD, “The Department of Defense Indo-Pacific Strategy Report.”
[17] Ibid.
[18] White House, “National Security Strategy.”
[19] White House, “Interim National Security Strategic Guidance.”
[20] Australian Signals Directorate (ASD), “Annual Report 2019–20.”
[21] Lewis, “US-Japan Cooperation in Cybersecurity.”
[22] US Air Force Assignment Management System, “Officer Authorizations”
[23] White House, “Joint Fact Sheet: The US-ROK Alliance”
[24] US Embassy Tbilisi, “US Helps Allies”; USCYBERCOM, “Estonia, US conduct Joint”
[25] Shanapinda, “How a Cyber Attack Hampered Hong Kong Protesters.”
[26] Ibid.
[27] Ibid.
[28] Chairman Joint Chiefs of Staff (CJCS), “Joint Publication 3-12.”
[29] DOD, “Department of Defense Cyber Strategy.”
[30] Kelly et al., *The U.S. Army in Asia.*
[31] DOD, “The Department of Defense Indo-Pacific Strategy Report.”
[32] Ibid.

Bibliography

Australian Signals Directorate. "Annual Report 2019–20." Australian Government; Australian Signals Directorate. Last modified 2020. https://www.asd.gov.au/sites/default/files/2020-10/asd-annual-report-2019-20.pdf.

Brimelow, Benjamin. "Fears of a Chinese Attack on Taiwan Are Growing, and Taiwan Isn't Sure Who Would Help if It Happened." Yahoo News - Latest News & Headlines. Last modified May 3, 2021. https://news.yahoo.com/fears-chinese-attack-taiwan-growing-125414441.html.

Chairman Joint Chiefs of Staff. "Joint Publication 3-12 (JP 3-12), Cyberspace Operations." Official Website of the Joint Chiefs of Staff. Last modified June 8, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

Department of Defense. "The Department of Defense Indo-Pacific Strategy Report." U.S. Department of Defense. Last modified June 1, 2019. https://media.defense.gov/2019/Jul/01/2002152311/-1/-1/1/DEPARTMENT-OF-DEFENSE-INDO-PACIFIC-STRATEGY-REPORT-2019.PDF.

_____. "Department of Defense Cyber Strategy." U.S. Department of Defense. Last modified 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Grossman, Derek. "China Has Lost the Philippines Despite Duterte's Best Efforts." RAND Corporation. Last modified May 6, 2021. https://www.rand.org/blog/2021/05/china-has-lost-the-philippines-despite-dutertes-best.html.

Kelly, Terrence K., James Dobbins, David A. Shlapak, David C. Gompert, Eric Heginbotham, Peter Chalk, and Lloyd Thrall. *The U.S. Army in Asia, 2030–2040*. Santa Monica: Rand Corporation, 2014. https://www.jstor.org/stable/10.7249/j.ctt1287mkz.10.

Lewis, James A. "US-Japan Cooperation in Cybersecurity." *Center for Strategic and International Studies*, November 2015. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151105_Lewis_USJapanCyber_Web.pdf.

Shanapinda, Stanley. "How a Cyber Attack Hampered Hong Kong Protesters." The Conversation. Last modified June 13, 2019. https://theconversation.com/how-a-cyber-attack-hampered-hong-kong-protesters-118770.

Shelbourne, Mallory. "Davidson: China Could Try to Take Control of Taiwan In 'Next Six Years'." USNI News. Last modified March 9, 2021. https://news.usni.org/2021/03/09/davidson-china-could-try-to-take-control-of-taiwan-in-next-six-years.

United States Cyber Command. "Achieve and Maintain Cyberspace Superiority Command Vision for US Cyber Command." Home USCYBERCOM. Last modified April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

_____."Estonia, U.S. Conduct Joint Defensive Cyber Operation." U.S. DEPARTMENT OF DEFENSE. Last modified December 3, 2020. https://www.defense.gov/Explore/News/Article/Article/2434474/estonia-us-conduct-joint-defensive-cyber-operation/.

US Embassy Tbilisi. "U.S. Helps Allies Fight Cyberattacks." U.S. Embassy in Georgia. Last modified August 26, 2020. https://ge.usembassy.gov/u-s-helps-allies-fight-cyberattacks/.

White House. "Interim National Security Strategic Guidance." The White House. Last modified March 2021. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

_____. "National Security Strategy." The White House – The White House. Last modified 2017. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Zheng, Sarah. "Australia Will Maintain Its Taiwan Policy, Prime Minister Scott Morrison Says." South China Morning Post. Last modified May 7, 2021. https://www.scmp.com/news/china/diplomacy/article/3132602/australia-will-maintain-its-taiwan-policy-prime-minister-scott.