China in the Asia-Pacific Cyber Domain

Okinawa and South China Sea case study

by Maj Dylan Buck

The United States must have a clear understanding of the operating environment in Asia-Pacific cyberspace. This domain has emerged as a militarized front and is where the "Chinese cyber dragon" will strike first if a conventional conflict were to emerge with the United States.[1] Some scholars propose that China watchers "may have missed the key development in cyber security: the shift from a state seeking to use cyber espionage [which accounts for approximately '78 percent of cyber exchanges between Beijing and its rivals']2 to catch up to its adversaries, to a state focused on maintaining dominance in the Asia Pacific."[3] The Chinese Communist Party's (CCP) lines of operation in the cyber domain consist of "deterrence through infiltration of critical infrastructure; military technological espionage to gain military knowledge; and industrial espionage to gain economic advantage."[4] Okinawa, Japan, and the South China Sea present two case studies into the emergence of China's militarized cyber operations in the Asia-Pacific. The case in Okinawa exhibits China's information warfare techniques aimed at advancing propaganda and amplifying social cleavages to propagate support for Chinese interests. China is more aggressive in the South China Sea, demonstrated by offensive cyber strikes perpetrated by Advanced Persistent Threat (APT) groups that utilize various tools intended to disrupt or deny access for public and private entities that challenge Chinese interests. China's strategic advantage over the United States in the Asia-Pacific is its centralized objectives in both public and private sectors that achieve synergy in the cyber domain. Moreover, its cybersecurity law enacted on 1 June 2017 requires network operators to store user data and allows the CCP uncontested access, establishing infinite avenues from which China can attack.[5] This article will discuss China's grand military strategy in cyber warfare by utilizing Okinawa and the South China Sea as microcosms.

>Maj Buck is an Infantry Officer currently studying National Security Affairs at the Naval Postgraduate School. He deployed in support of Operation Enduring Freedom and the Unit Deployment Program.

China's Grand Cyber Strategy

China's more recent foreign policy endeavors seek to challenge sovereignty norms in Asia; the means have been concentrated in cyberspace.[6] According to Taylor Fravel, a well-recognized China scholar, China's latest military strategy focuses on "informatization warfare," or "*xinxihua,*" the application of information technology to all aspects of military operations.[7] China has identified that key objectives in future "military struggle will be placed on winning informatized local wars."[8] Its cyber strategy is "intrinsically link[ed] to information warfare doctrines."[9] The People's Liberation Army (PLA) defines the "informationized war" as

> decision control warfare, where information is the main weapon designed to attack the enemy's cognitive and information systems and influence, contain or change the decisions of enemy policy makers.[10]

Michael Pillsbury, author of *The Hundred-Year Marathon*, and Graham Allison, of *Destined for War*, reference China's strategy of *Shih*, analogous to the United States military's concept of the center of gravity. China's operations focus on "subtle shifts in momentum and relative advantage" by waging "information warfare on behalf of the nation ... to cultivate changes in the strategic landscape."[11] It is through the cyber domain that China is surging intellectual and material capital to shape the operating environment in the Asia-Pacific. While its tactics may not be garnering as much popular support in the Asia-Pacific, China is achieving its aims through coercion imposed on those who challenge its interests. It leverages its robust suite of cyber capabilities to impose diplomatic, economic, information, and military retribution.

Chinese military theory contends that warfare has transitioned "from the Industrial Age to the Information Age"[12] and had demonstrated this strategic operational shift through its creation of the Strategic Support Force (SSF). The SSF, established in 2016, is the PLA's operating arm in cyberspace and reports directly to the Central Military Commission—independent from any theater-level military commands.[13] The SSF executes the PLA space, cyber, electronic, and psychological warfare objectives. Chinese military leaders have declared that the information battle is the decisive objective in future conflicts and that the initial salvos will be launched in the cyber domain.[14] The SSF operates in the nebulous zone between peacetime and wartime to achieve "escalation dominance, a condition wherein China maintains the initiative in shaping adversary behavior in a crisis scenario that has not yet become a full-on conflict."[15]

China's Tactics in Okinawa

The U.S. military maintains roughly 40 percent of its military forces in Japan on the island of Okinawa; the island has become a target for China's emergent information operations in the cyber domain.[16] China's recent information warfare strategy in Okinawa has been to attack Japan's sovereignty over the prefecture and escalate "local opposition to U.S. military bases in Okinawa, and animosity towards the Japanese central government."[17] For the People's Republic of China, it has "an eye on the long game, building links between malcontents in Okinawa and patriots in Hong Kong [that] could easily pay off in the future."[18] The information war is waged through various media outlets that are agents of the SSF and operate in Okinawa through the United Front Work Department (UFWD) or as Chines President Xi Jinping refers to it: "China's magic weapons."[19] The principle UFWD branch in Okinawa is the Organizing Committee for the Ryukyu Islands Special Administrative Region of the Chinese Race. This organization operates off the SFF's information warfare doctrine to engage in "Three Warfares: public opinion warfare, psychological warfare, and legal warfare."[20] The battlefield for the "Three Warfares" in Okinawa exists in the cyber media domain. (See Figure 1.)

In a 2015 article in *Foreign Affairs*, David Shambaugh estimated that the Chinese government spends over ten billion dollars annually on propaganda in foreign countries.[21] According to the U.S. China Economic and Security Review Commission, the UFWD is the CCP's agent for political interests abroad and is highly resourced and tasked with "gain[ing] influence that is interwoven with sensitive issues such as ethnic, political, and national identity,"[22] to either co-opt or coerce CCP opposition. Like the SSF, the UFWD reports directly to the Central Military Commission and the two organizations operate jointly and to target social, commercial, academic, and political elites abroad.[23] The UFWD utilizes various forms of media platforms to "influence, disrupt, corrupt, [and] usurp the decision making"[24] of the Okinawan government and citizens. Messaging is implemented through public blogs, social networks, and online postings by UFWD agents.[25] The UFWD exploits "anti-Japanese sentiment in Okinawa itself, where both political leaders and the local media are antagonistic toward Tokyo."[26] One tactic utilized to exploit such sentiments is through propaganda aimed at amplifying ethnic cleavages to encourage independence from Japan. The president of the Okinawan UFWD, Zhao Dong, posted in 2015 that the Ryukyus should become part of China because "[t]he Japanese people are a part of the Chinese race and Japan is originally of Chinese blood."[27] Another divisive social media post in Okinawa exclaimed, "The Chinese race is relying on you. The Chinese race today relies on you, and the Chinese race can rely on you."[28]

Scholars at the Johns Hopkins School of Advanced International Studies (SAIS) recently discovered that Chinese cyber operatives create massive numbers of social media accounts to gain access in places of military strategic interest.[30] Twitter, Japan's second most popular social media platform, is one of the UFWD's primary platforms for CCP propaganda.[31] There are over one million employed in China's cyber business who promote propaganda, regulate the internet, censor freedom of speech, and hack infrastructure to execute informationalized intimidation.[32]

Willy Lam, a political science expert at the Chinese University of Hong Kong, argues that China's social media campaigns seek to apply pressure on the Okinawa issue to raise the stakes of territorial disputes in the East and South China Sea. Lam specifically asserts, "this is psychological warfare. The major point is to put pressure on Japan so that the Japanese administration will be forced to make concessions over the Senkaku islands."[33] The Japanese Intelligence Agency reinforced Lam's claim by pointing to an article published by the *Global Times* that argued for the international community to refer to Okinawa as Ryukyu, the name of the island when it paid tribute to the Ming Dynasty of China in the 14th century.[34] Further challenges to the island's sovereignty came from a retired PLA general who stated, "I am not saying all former tributary states belong to China, but we can say with certainty that the Ryukyus do not belong to Japan."[35] The Japanese Public Security Intelligence Agency recently exposed efforts by Chinese universities and think tanks that were targeting Japanese academic institutions

Type of Approach

Target	Defensive	Offensive
Chinese	• Promoting government narratives • Reaffirming Party legitimacy through nationalism • Outreach to overseas Chinese • Enforcing the Party line abroad • Attacking regime opponents abroad	• Extending judicial reach • Intimidation through surveillance
Foreign	• Promoting government narratives • Enforcing the Party line abroad	• Military strategic messaging • Extending judicial reach • Spreading fake news

Figure 1. Taxonomy of Chinese influence operations via social media.[29]

to co-opt support over Okinawa by providing research grants and other types of funding to intensify public divide. The intelligence agency asserts the attempts were intended to "swing public opinion in [China's] favor [to] spark a split with Japan."[36]

On June 2020, the United States officially labeled China Central Television, the China News Service, the *People's Daily* and the *Global Times* as "propaganda outlets" of the CCP.[37] The UFWD and other Chinese agents have an army of social media accounts on various platforms (see Figure 2) that post and retweet CCP propaganda that specifically target partisan and ethnic cleavages in Okinawa.[38] An academic journal associated with the Chinese Ministry of Foreign Affairs, *Shijie Zhishi*, proclaimed in July 2013, "The Ryukyus were China's territory from long ago; Japan stole them and the Diaoyu Islands [Senkaku] by military force and under U.S. protection."[39] In addition, the *Global Times* followed up by declaring, "If Japan seeks to be a pioneer in sabotaging China's rise, China can carry out practical input, fostering forces in Okinawa that seek the restoration of the independence of the Ryukyu Chain."[40] Such statements are posted, tweeted, re-tweeted, and proliferated in a synchronized fashion across China's numerous social media accounts.

China has also sought to gain a cyber foothold in Okinawa through infrastructure that is gained through economic development. The method for initiating these economic partnerships is by increasing the "number of sister-city relationships formed between Chinese cities and Okinawa."[42] The "sister-city" linkage has become known as Beijing's method for advancing soft power objectives, but it is becoming more apparent these partnerships are an apparatus for embedding infrastructure. In 2019, Prague voted to remove the sister-city status with China after financial corporations accused the CCP of pressuring companies to "spread pro-PRC [People's Republic of China] propaganda." Moreover, the Czech cyber security agency NUKIB warned of further Chinese coercion if Huawei equipment was utilized at critical nodes

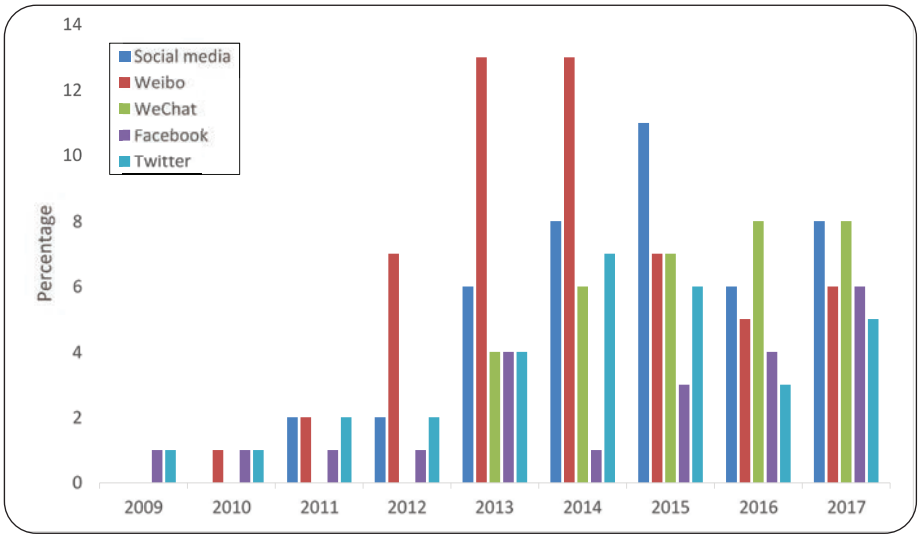

Figure 2. Articles on Chinese diaspora and social media in international communications.[41]

of the country's telecommunications infrastructure.[43] Many cyber security firms, to include the U.S. National Security Agency, allege Huawei is an asset for CCP cyber espionage. As of 2018, Huawei reported receiving a U.S. $100 billion line-of-credit from Chinese state-owned banks.[44]

In February 2018, the United States CIA, FBI, and NSA issued warnings that the public should cease using products supplied by Huawei and ZTE.[45] Both of these companies are alleged to serve as backdoors for Chinese espionage and cyberattacks. Huawei recently "unveiled a suite of new solutions to help Internet Service Providers revamp Internet infrastructure in Asia Pacific."[46] In Okinawa, Huawei owns 3 of the 6 submarine cable lines that provide internet to Okinawa, and approximately 99 percent of all international internet traffic is transmitted through submarine cables.[47] It is well established that "Chinese law gives the government sweeping authority to compel private businesses to support intelligence operations,"[48] and that Huawei is beholden to such requirements. Furthermore, it is speculated that Huawei is a Chinese state-owned enterprise. Donald Clarke, of George Washington University, and Christopher Balding, of Fulbright University Vietnam, discovered that Huawei "is wholly owned by a holding company, of which 99 percent is held by an entity called a 'trade union committee.'"[49] These scholars suggest this presents credible evidence that Huawei could be indirectly owned by the CCP.

China's Tactics in South China Sea

Significant attention is attributed to China's naval aggression in the South China Sea, yet what inflicts vastly superior material damage in the region is China's cyberattacks on public and private enterprises. FireEye, Securelist, and CrowdStrike, three of the world's leading cybersecurity firms, reported in 2015 that China infiltrates public and private sectors in the South China Sea to "gain [a] strategic edge over its regional rivals," and then attacks those who contest their sovereignty claims as stipulated in China's illegal Nine-dash line.[50] In the South China Sea, Chinese cyberattacks "target critical military and civilian nodes to deter or disrupt adversary intervention, and to retain the option to scale these attacks to achieve desired conditions with minimal cost."[51] China's escalated naval provocations in the South China Sea tend to be preceded by attacks in the cyber domain. The PLA has been associated with private sector high-tech firms, freelance hackers, and students at elite universities to attack adversary logistics and command and control assets in the South China Sea.[52]

Chinese hackers in the South China Sea predominately utilize spear phishing, watering hole, and malware

tools to attack actors who challenge Chinese interests.[53] Advanced Persistent Threat (APT) 30, also known as Naikon, PLA Unit 78020, and Lotus Panda, has customized malware in the form of SHIPSHAPE, SPACESHIP, and FLASHFLOOD that exploit vulnerabilities from air-gapped computers to gain remote access to victims' networks and hardware.[54] Kaspersky Lab, a leading cybersecurity firm, has attributed attacks in the Philippines, Malaysia, Cambodia, Indonesia, Vietnam, Myanmar, Singapore, and Nepal to APT30. The lab notes that the malware attacks target "military, government, and civil organizations located in and around the South China Sea." The lab further identified that in one country, which it declined to name, APT30 "compromise[d] the Office of the President, Military Forces, Office of the Cabinet Secretary, National Security Council, Office of the Solicitor General, National Intelligence Coordinating Agency, Civil Aviation Authority, Department of Justice, Federal Police and Executive/presidential Administration and Management Staff."[55]

FireEye reported in 2018 that another prominent group that targeted operations in the South China Sea was APT10. APT10 is "primarily tasked with collecting critical information in response to shifts in regional geopolitics and frequently targets organizations with long research and development cycles."[56] In December 2018, the United States Department of Justice issued a statement that APT10 had violated U.N. Charter Article 2(4) as it

> acted in association with the Chinese Ministry of State Security ... [and] engaged in an intrusion campaign to obtain unauthorized access to computer networks of commercial and defense technology companies and U.S. Government agencies in order to steal information and data concerning a number of technologies.[57]

Furthermore, FireEye recently reported that APT10 frequently attacks U.S. engineering and defense companies that operate in the South China Sea to obtain sensitive information about radar systems and their arch ranges.[58] APT10 generally utilizes spear phishing tools to gain access to U.S. and Japanese network providers that are known to service defense and government entities.[59] APT10 has utilized "'AIRBREAK,' a JavaScript-based backdoor [and] 'BADFLICK,' a backdoor for changing command and control (C2) configuration."[60] It has also been connected with "deploy[ing] two malicious software variants that targeted government and private organizations in the Philippines" in 2019.[61] APT10 purposely hacked the Philippines' military websites by inserting malicious scripts that captured users' information who accessed the websites. The 2019 APT10 attacks were followed by "275 Chinese maritime militia vessels, complemented by the Chinese Coast Guard, in the waters around Philippine-controlled Pag-Asa Island."[62] China's combined arms of cyber and naval actions in the South China Sea present an overwhelming dilemma to its victims.

Conclusion

China's advantage in the Asia-Pacific is attributed to the synergistic effects it achieves in synchronizing its diplomatic, information, military, and economic interests through cyber means. The CCP's recent tactics expand beyond espionage and efforts to steal intellectual property and have evolved into more offensive measures to swing popular opinion in Okinawa to disrupt/deny public and private enterprise in the South China Sea. China's unity of command and capacity to leverage combined arms utilizing cyber presents a dilemma to the Unites States in the region. Its advantages are enhanced with its 2017 cyber law that delivers unlimited avenues to virtually every network and piece of hardware operating in the Asia-Pacific. Its capacity to "leverage cyber tools for economic, commercial, and technological advantage only confirms the pessimist's worst fears: a war with China that starts in the digital domain but ends in World War III."[63] Michael Pillsbury predicts:

> once China is strong enough economically and militarily to defy the United States and its allies, Chinese officials could use cyberattacks to harass anyone whose speech they disapprove of; many people outside of China, from Asia to North America, would consequently have to watch what they say and wonder whether they will be punished.[64]

Notes

1. Dean Cheng, *Cyber Dragon, Inside China's Information Warfare and Cyber Operations*, (Santa Barbara, CA: Praeger, 2016).

2. Brandon Valeriano, Benjamin Jensen, and Ryan Maness, *Cyber Strategy*, (New York, NY: Oxford University Press, 2018).

3. Ibid.

4. Magnus Hjortadal, "China's Use of Cyber Warfare: Esponage Meets Strategic Deterrence," *Journal of Strategic Security*, (Milton Park: Routledge, Summer 2011).

5. Jack Wagner, "China's Cybersecurity Law: What You Need to Know," *The Diplomat*, (June, 2017), available at https://thediplomat.com.

6. *Cyber Strategy*.

7. Taylor Fravel, *Active Defense*, (Princeton, NJ: Princeton University Press, 2019).

8. Ibid.

9. *Cyber Strategy*.

10. Ibid.

11. *Cyber Strategy*; Graham Allison, *Destined for War*, (New York, NY: Mariner Books, 2017); and Michael Pillsbury, *The Hundred-Year Marathon*, (New York, NY: Henry Holt and Company, 2015).

12. *Active Defense.*

13. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," *Institute for National Strategic Studies*, (Washington, DC: National Defense University Press, 2018).

14. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2019,* (Washington, DC: 2019).

15. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," *Institute for National Strategic Studies*, (Washington, DC: National Defense University Press, 2018).

16. Catherine Lutz, *The Bases of Empire: The Global Struggle against U.S. Military Posts*, (New York, NY: New York University Press, 2009).

17. Russell Hsiao, "A Preliminary Survey of CCP Influence Operations in Japan," *The Jamestown Foundation*, (June 2019), available at https://jamestown.org; and Staff, "Japan Slams Alleged China-Based Hackers After Cyberattacks On Government, Firms and Colleges," *The Japan Times*, (December 2018), available at https://www.japantimes.co.

18. Larry Diamond and Orville Schell, *China's Influence & American Interests: Promoting Constructive Vigilance*, (Stanford, CA: Hoover Institution Press, 2019).

19. Michael Mazarr et al., *Hostile Social Manipulation*, (Santa Monica, CA: RAND, 2019).

20. Jason Morgan, "Is Japan Putting Up A Good Enough Fight Against China's Propaganda Warfare?" *Japan Forward*, (August 2020), available at https://japan-forward.com.

21. David Shambaugh, "China's Soft-Power Push," *Foreign Affairs*, (July 2015), available at https://www.foreignaffairs.com.

22. Alexander Bowe et al., "China's Overseas United Front Work: Background and Implications for the United States," (Washington, DC: U.S.-China Economic and Security Review Commission, August 2018).

23. Clive Hamilton, *Silent Invasion: China's Influence in Australia*, (London: Hardi Grant, 2018).

24. Joint Chiefs of Staff, *Publication 3-13, Information Operations*, (Washington, DC: Department of Defense, 2012).

25. *China's Influence & American Interests.*

26. Ibid.

27. Ibid.

28. Ibid.

29. *Hostile Social Manipulation*.

30. Fergus Ryan, "China's Online Warriors Want More Gates in the Firewall," *Foreign Policy*, (June 2020), available at https://foreignpolicy.com.

31. Selina Wang, "How Twitter Became Ubiquitous in Japan," *Bloomberg*, (May 2019), available at https://www.bloomberg.com; and "China's Overseas United Front Work."

32. *The Hundred-Year Marathon*.

33. Agence France Presse, "Now China Says it May Own Okinawa, Too," *Business Insider*, (May 2013), available at https://www.businessinsider.com.

34. Isabel Reynolds, "Japan Sees Chinese Groups Backing Okinawa Independence Activists," *Bloomberg*, (December 2016), available at https://www.bloomberg.com.

35. *China's Influence & American Interests*.

36. "Japan Sees Chinese Groups Backing Okinawa Independence Activist."

37. David Brunnstrom, and Humeyra Pamuk, "U.S. Designates Four Major Chinese Media Outlets as Foreign Missions," *Reuters*, (June 2020), available at https://www.reuters.com.

38. *China's Influence & American Interest.*

39. Nagamoto Tomohiro, "Who 'Owns' Okinawa," *Nippon*, (July 2013), available at https://www.nippon.com.

40. Ibid.

41. *Hostile Social Manipulation*.

42. Russell Hsiao, "A Preliminary Survey of CCP Influence Operations in Japan," *The Jamestown Foundation,* (June 2019), available at https://jamestown.org.

43. Martin Hala, "Making Foreign Companies Serve China: Outsourcing Propaganda to Local Entities in the Czech Republic," *The Jamestown Foundation*, (January 2020), available at https://jamestown.org.

44. Andrew Grotto, "The Huawei Problem: A Risk Assessment," *Global Asia*, (September 2019), available at https://www.globalasia.org; and Shinichi Hirata, "2019 Annual Cybersecurity Report," *NTT-CERT*, (September 2019), available at https://www.ntt-cert.org.

45. "2019 Annual Cybersecurity Report."

46. Staff, "Huawei Unveils New Solutions to Revamp Asia Pacific Internet Infrastructure for AI and 5G Connectivity," *Huawei Enterprises,* (March 2019), available at https://e.huawei.com.

47. David Brown, "10 Facts About the Internet's Undersea Cables," *Mental Floss,* (November 2015), available at https://www.mentalfloss.com.

48. "The Huawei Problem: A Risk Assessment"; "2019 Annual Cybersecurity Report."

49. Wei Sheng, "Huawei's Clam Of 100% Employee Ownership Is False, May Be State-Owned," *Technode*, (April 2019), available at https://technode.com.

50. Anni Piiparinen, "The Chinese Cyber Threat in the South China Sea," *The Diplomat*, (September 2015), available at https://thediplomat.com.

51. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2019*, (Washington, DC: 2019).

52. Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground," *International Journal of Computer Research*, (GSSRR, 2014).

53. Marie Baezner, "Hotspot Analysis: Use of Cybertools in Regional Tensions in Southeast Asia," (Zurich: CSS, 2018).

54. "Hotspot Analysis"; and Staff, "Advance Persistent Threat Groups," *FireEye*, (2020), available at https://www.fireeye.com.

55. Brian Donohue, "Naikon APT Steals Geopolitical Data from the South China Sea," *Kaspersky Daily*, (May 2015), available at https://www.kaspersky.com.

56. David Tweed, "China Cyberspies Mined Japanese Firms for North Korean Secrets," *Bloomberg*, (April 2018), available at https://www.bloomberg.com.

57. LT Jason Bently and LTJG Brandon Maitlen, "Cybersecurity in Southeast Asia: Deterring China's APT10," *Bengoshi*, (2019), available at https://www.jag.navy.mil.

58. "2019 Annual Cybersecurity Report."

59. "Advance Persistent Threat Groups."

60. "2019 Annual Cybersecurity Report."

61. Mark Manantan, "The Cyber Dimension of the South China Sea Clashes," *The Diplomat,* (August 2019), available at https://thediplomat.com.

62. Ibid.

63. *Cyber Strategy.*

64. *The Hundred-Year Marathon*.