Leveraging Ally and Partner Nation Intelligence, Surveillance and Cyber Capabilities to Defend Against the Taiwan Scenario

Captain Bria McClary

USAF SOS Class 21E B19

Disclaimer: Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air Force Research Institute, Air University, the United States Air Force, the Department of Defense, the United States Strategic Command, or any other US government agency.

Leveraging Ally/Partner Nation Capabilities to Defend Against the Taiwan Scenario

The People's Republic of China (PRC) tempts its neighbors with sweet words for their support and sharp consequences if rejected. Critical aspects of the global market and considerable aid to less affluent keep the PRC relevant and necessary. They are a serrated blade hidden in a velvet sheath that does not care for US interests over their own nor the current powerbase and they ensnare others in obligations, regardless of international discontent. How do you limit such a power when they narrowly contain themselves to the grey zone - a competitive space that does not yet cross into the domain of war but presses strategic efforts [28]? One avenue is through integrative and expansive intelligence, surveillance, and reconnaissance efforts between nations. This effort can be honed through establishing trust between our partner nations and allies, proper supply efforts for ISR/Cyber readiness, and training initiatives that streamline data collection, interpretation, and dissemination.

In preparation for the next conventional war, Washington must adjust its fighting strategy against the actions of the PRC who stoutly defends its right to both Taiwan and the South China Sea [32][3]. If Washington aims to intercede in Chinese influence, they cannot do it alone and the possibility of war is not one to be ignored [1]. China's access to resources is hemmed in by Taiwan, the Philippines, and Japan [5]. Despite the PRC's overwhelming anti-access/areal denial capabilities, the resources they depend on to sustain their population and infrastructure appear vulnerable when they travel through the waterways between these nations [25][10]. Continued clashes over control of this region push the area to armed conflict and proper preparation for this potentiality highlights the need to collect partners [28]. Our closest allies IVO China are South Korea, Japan, New Zealand, and Australia [19]. Additionally, we have strong working relationships with Taiwan, Singapore, Malaysia, Indonesia, and the Philippines but we are improving international relations with Vietnam, Thailand, and India [10]. To gain and maintain access to the resources and information network of these countries, Washington must be more deliberate politically, economically, and/or socially while balancing the conflicting histories of those same partners.

Washington's aims to limit China can be codified into the DIME domain (Diplomacy, Information, Military, Economics) [24]. Through information and military support, opportunities to coordinate with partners emerge in both diplomatic and military avenues. For example, we know China has cemented itself as an economic pillar in the 21st century. It supplies coal, agricultural stock, and rare earth minerals to dozens of countries and manages 7.86 trillion dollars in foreign financial assets [31][7]. However, due to the rapid drive for industrial modernization, China relies on other countries for construction imports from the global market. Over 85% of all Chinese foreign trade is conducted by ship and the SCS is the means to transport it [30][32]. This dynamic is highly impactful in a diplomatic lens. Reliance on Chinese exports and intakes influences the geopolitical stage great deal and individual nations can suffer significantly if they remain obstinate as the PRC works to optimize and improve their stability through domination of the South China Sea (SCS) [3]. Domination allows the PRC can maintain their vital shipping routes and achieve regional reach despite infringing on the security of the nations surrounding it. This discontent allows Washington an avenue of approach to coordinate ISR/cyber capabilities. Information sharing and cooperation is a prudent option to remain aware of China's actions and intentions, without crossing the line to outright conflict, while remaining poised for rapid response should the PRC's actions continue to escalate from missile demonstrations and harassment of other sea vessels [5]. Through them, Washington can engage a proactive, rather than reactive, strategy. Through DIME efforts, policies can be implemented that better strengthen these ties.

The US has maintained diplomatic and military ties with their partner nations through several ways. Exercises that encourage trust and mutual benefit can strengthen bonds; humanitarian efforts and aid highlight the desire to assist; and information exchanges that protect partners and allies from an internal or external threat presents our willingness to act instead of simply assuring change. Explicit examples include international Exercises like KEEN SWORD and COBRA GOLD, which demonstrate our willingness to support and enhance our partners for the betterment of both their people and the region [13][14]. Here cyber defense, communication and control (C2), joint defense, and humanitarian and disaster response forces are tested in robust scenarios. The lessons learned in these forums are used to better prepare for real world military interoperability. Additionally, diplomatic efforts have managed to bolster ISR resources in South East Asia and surrounding lands over the past two years.

Reconnaissance purchases have increased in India and the Philippines, as well as defensive hardware requests from Australia, South Korea and Japan, offering fruitful avenues for military readiness [11]. Australia and Taipei's Economic and Cultural Representative Office (TECRO) procured MQ-9s for recon efforts while India purchased 6 P-8 Poseidon aircraft for use in monitoring their controlled airspace. Australia will also supplement their Intelligence, Surveillance, and Reconnaissance efforts through MQ-4C Triton and P-8 Poseidon aircraft [2]. With recently gained pod improvements, their enhanced imagery exploitation software, shortened sensor to shooter timelines and multispectral imaging can allow for detailed and near-realtime updates of PRC movements and efforts [9]. These ISR mechanisms can provide the edge needed to quickly responds to PRC aggression. Similarly, use of various imagery and radar satellites in lower earth orbit is a capability utilized by both China and the United States and India has placed attention to improving their space resources. They have considered budget to generate small satellites (SmSats) whose smaller cost and low orbit could set the foundation for their monitoring of Chinese mechanizations. With the proper support, SmSats could replicate or rival Chinese constellations that, when used conjointly with imagery satellite, provide a comprehensive picture of enemy military movements and coordination [6]. The rapid deployment and increased flexibility for communications, imagery, reconnaissance, and surveillance offer worthwhile benefits for those using the model and an opportunity to expand Washington interests in the region for military efforts should the environment shift to true combat [29]. Namely, additional satellite constellations for datalink reach could expand military or commercial usage without personally dedicating US assets.

Conversely, utilizing existing ISR assets to coordinate military action is not the only potential option. They can also be used to inform diplomatic decisions or responses. In fact, much can be learned from the cyber actions that have already been accomplished against perceived threats to the PRC. For example, Beijing has an unquestionably robust cyber and intelligence capability, and they are effective in using it to their advantage [12]. The PRC's military arm has been implicated in the information leaks of 115 US enterprises due to their innovate stance on cyber warfare [27]. They have successfully infiltrated Japanese, Taiwanese and US information networks through both private and militarized hacking efforts. In this way, they can capture sensitive data on technological items to meet their goals of technological superiority [25]. This is militarily troubling because network paralysis could disrupt country infrastructures for energy, hospitals and water supplies. A chilling prospect for homestation. In the diplomatic realm, cyber can be just as devastating. Efforts to discredit and influence the population through internet nodes is also a means of shifting the balance of power to a pro-PRC leaning and defenses to combat this must be multifaceted [27]. It requires monitoring of social networks and public opinion; identifying sources that influence or bias the population; offering countermeasures or PA reps to push the narrative; and honest cooperation to improve defense and identify attacks. Supporters in limiting PRC influence should compile and disseminate best practices to protect against information theft, disinformation, or malicious soft actions [17]. We've already seen examples of successful partnerships in this endeavor. The EU Hybrid Center of Excellence shared information practices that bolster EU security. An Asian alternative was considered during the 2018 Association of Southeast Asian Nations (ASEAN) summit. There, initiatives to train and research cybersecurity threats were discussed [26]. Through strengthening the cyber capabilities of all members, attacks can be better routed as they strive for equality of defense [4][26].

Once the capabilities of potential allies are considered, barriers to gaining those resources are next to contend with. Pooling resources to analyze and innovate is a measure that can enhance partner interoperability and trust. However, gaining the trust of each nation while ensuring they trust their fellow members is likely to be a difficulty. Ignorance to the tensions present is an excellent way to alienate potential partners. Managing the conflicting relationships in the South East Asia is a mammoth task, but entering negotiation with these conflict in mind can only strengthen our arguments to sustain and mold lasting cooperation. Fortunately, China's actions to consolidate their own power has alienated the region enough to turn them against the bigger threat instead of antagonizing one another [25]. Even so, those nation's trust in Washington can be strained as demonstrated in Filipino President Rodrigo Duerte's February 2020 announcement to terminate the Visiting Forces Agreement, a pact that has stood for over two decades. He admitted the decision was influenced by a lack of faith in Washington's commitment to the defense of the Philippines and stability of the Indo-Pacific region [23]. Loss of this strategic pact could jeopardize efforts to successfully combat Beijing aggression. Clearly, conflicting, self-interested needs degrade collaborative efforts and lasting alliances have been difficult to maintain on the previous foundations [8]. To combat this, initiatives like the quadrilateral dialog require transparent cooperation, mutual security of intelligence assets, and unified goals to allow for effective partnerships against the PRC's reach [8][17][25].

The final point to consider is how best to employ ISR and cyber capabilities through diplomatic and military means. The sharing of satellite constellations or interchanges of data from the satellites overhead can provide increased awareness on China's movements in the SCS. Satellite imagery has already shown the sudden increase of People's Liberation Army (PLA) missile silos, possible bunkers along the China/India border, and Uyghur incarceration camps hidden away in the nation's desert [15][16][18]. A fortified satellite network that can withstand the multi-dimensional needs of air, ground and space networks can support the growing demand for Unmanned Arial Vehicles and provide additional information on locations of interest to provide both diplomatic pressure and inform military response [6]. Both Australia, India and Taiwan have invested heavily in the UAV market to supplement their ISR needs, and it also provides an offset tool for monitoring PRC activity [11]. Employing their capabilities allows for reduced cost with US forces and diverse sources to verify and highlight points of concern. But the most critical thread in a joint efforts is ensuring everyone is on the same page. Washington could offer training to hone other's ISR employment and maximize the tools on hand for better information gathering. Already our exercises push their militaries to fight like we do, but we must enhance how they think and process data too. Training initiatives that incorporate real time analysis of data as it is collected through the method of processing, exploitation, and dissemination (PED) is a proven tactic that has expedited decision making in both combat efforts and humanitarian aid [33]. Joint cyber campaign exercises like Cyber Storm can highlight partner weak points as well as generate defense to unique attacks [4]. Collaborating in this way can ensure our actions are trusted for their authenticity in strengthening their country. Should we continue this effort, we must ensure information is isolated and compartmentalize to prevent leaks or exposure for vulnerable native assets. Finally, we must share in both our experience and our knowledge to best leverage capabilities outside of US control.

While the PRC aims to strengthen its hold on the region, it is not a malicious effort but a plan to secure their nation as it struggles through internal difficulties [20][21][22]. Their efforts can be consolidated into economic security through the SCS, superiority in technological developments, increased military projection for its forces, and a rejuvenation and reconsolidation of Chinese ancestral holdings [12]. Through leveraging ally and partner nation ISR/Cyber capabilities, these goals can be mitigated or monitored. The PRC's attempts to retain their economic security through militarizing shoals in the South China Sea requires aggressive ISR cooperation to assess their capabilities and weaknesses while limiting obscuration efforts in the region. Undermining military projection requires accurate and rapid updates on the situation at hand so US assets and ally/partner nations remain aware of the potential threat. Proper supply and training maximize the success of this effort. Reducing superiority in technological theaters demands active and vigilant cyber defense to prevent technologies from being intercepted by rival nations. Finally, rebutting the consumption of the neighboring nations requires deliberate interactions between historically opposed peoples and diligent excision of misinformation campaigns. Initiatives like the quadrilateral dialog can be a means to collaborate ISR/cyber capabilities but it requires transparent cooperation, mutual security of intelligence assets, and unified goals to allow for effective partnerships against the PRC's reach. For now, we are making worthwhile strides in building the necessary trust to best utilize the tools at hand. In time we shall see how far these relationships shall grow.

References

1. Asia Society. (2018). “Destined for war: can America and china escape Thucydides’ trap” *YouTube.* https://www.youtube.com/watch?v=_gPoXwD_Jj8

2. Australian Government Department of Defence. (2016). “2016 Defence white paper”. https://www.defence.gov.au/Whitepaper/AtAGlance/ISR-Cyber.asp

3. BBC. (26 May 2021). “What’s behind the china-taiwan divide?”. *British Broadcasting Corporation (BBC) News.* https://www.bbc.com/news/world-asia-34729538

4. BBC. (4 November 2019). “US and Taiwan hold first joint cyber-war exercise”. *British Broadcasting Corporation (BBC) News.* https://www.bbc.com/news/technology-50289974

5. Bengali, S. & Bou Uyen, V. (2020). “Beijing’s aggressive South China Sea expansion shows its willingness to defy international law for president Xi Jinping’s visions of power”. *Los Angeles Times.* https://www.latimes.com/world-nation/story/2020-11-12/china-attacks-fishing-boats-in-conquest-of-south-china-sea

6. Bommakanti, K. (2020). “Strengthening the C4ISR capabilities of India’s armed forces: The role of small satellites.” *Observer Research Foundation*, *254*. https://www.orfonline.org/research/strengthening-the-c4isr-capabilities-of-indias-armed-forces-the-role-of-small-satellites-67842/

7. Brodzicki, T. (25 February 2020). “Agri-food exports of china” *IHS Markit*. https://ihsmarkit.com/research-analysis/agrifood-exports-of-china.html

8. CaspianReport. (2021). “The making of an Asian NATO”. *YouTube.* https://www.youtube.com/watch?v=SvabgXS6gZQ

9. Collins Aerospace. (2021). “Advanced, long-range day/night reconnaissance.” https://www.

collinsaerospace.com/what-we-do/Military-And-Defense/Avionics/Surveillance/Airborne-Reconnaissance

10. Council on Foreign Relations. (2021). “U.S. relations with China”. https://www.cfr.org/timeline/us-relations-china

11. Defense Security Cooperation Agency. (2021). *Department of Defense Security Cooperation Agency.* https://www.dsca.mil/press-media/major-arms-sales

12. Department of Defense. (2020). “Military and security developments involving the people’s republic of China 2020” *Annual Report to Congress*. https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF

13. GlobalSecurity.org. (2021). https://www.globalsecurity.org/military/ops/cobra-gold.htm

14. GlobalSecurity.org. (2021). https://www.globalsecurity.org/military/ops/keen-sword.htm

15. Griffiths, J. (4 November 2020). “Satellite images appear to show china developing area along disputed border with India and Bhutan”. *CNN.* https://www.cnn.com/2020/11/24/asia/china-india-bhutan-doklam-intl-hnk/index.html

16. Irving, D. (2021). “China’s disappeared Uyghurs: What Satellite images reveal.” *RAND Review.* https://www.rand.org/blog/rand-review/2021/04/chinas-disappeared-uyghurs-what-satellite-images-reveal.html

17. Kroenig, M., Cimmino, J., Casarini, N., Fukushima, A., Jain, A., Kirchberger, S., Medcalf, R., Mohan, C. R., Nicholas, F., Paris, R., Patalano, A., and Woo, J. (2020). "Global strategy 2021: An allied strategy for China". Atlantic Council. https://www.atlanticcouncil.org/global-strategy-2021-an-allied-strategy-for-china/

18. Lendon, B. (2021). “China is building a sprawling network of missile silos, satellite imagery

appears to show”. *CNN.* https://www.cnn.com/2021/07/02/asia/china-missile-silos-intl-hnk-ml/index.html

19. Office of the Historian. (2021). “Countries”. *United States Department of State.* https://history.state.gov/countries

20. PolyMatter. (2021). “Demography – China’s Reckoning (Part 1)” *Youtube.* https://www.youtube.com/watch?v=vTbILK0fxDY

21. PolyMatter. (2021). “Housing – China’s Reckoning (Part 2)” *Youtube.* https://www.youtube.com/watch?v=EgVXRtq5EIg

22. PolyMatter. (2021). “Water – China’s Reckoning (Part 3)” *Youtube*. https://www.youtube.com/watch?v=nRUc4gTO-PE

23. Reuters. (14 June 2021). “Philippines delays scrapping of US visiting forces agreement”. *CNN.* https://www.cnn.com/2021/06/14/asia/philippines-us-visiting-forces-agreement-intl-hnk/index.html

24. Rodriguez, C. A., Walton, T. C., & Chu, H. (2020). “Putting the “FIL”into“DIME”: Growing joint understanding of the instruments of power”. *Washington Headquarters Services.* https://www.whs.mil/News/News-Display/Article/2133177/putting-the-fil-into-dime-growing-joint-understanding-of-the-instruments-of-pow/

25. Scobell, A., Burke, E. J., Cooper II, C. A., Lilly, S., Ohlandt, C. J. R., Warner, E., & Williams, J. D. (2020). “China’s grand strategy: Trends, trajectory, and long-term competition.” *RAND Corporation.* https://www.rand.org/pubs/research_reports/RR2798.html

26. Segal, A. Akimenko, V., Giles, K., Pinkston, D. A., Lewis, J. A., Barlett, B., Huang, H, &

Noor, E. (2020). “Roundtable: The future of cybersecurity across the asia-pacific”. *Asia Policy, 15*(2), pp. 57-114. https://www.nbr.org/wp-content/uploads/pdfs/publications/ap15-2_cyberrt_apr2020.pdf

27. Shen, M. (2019). “China’s cyberwarfare strategy and approaches toward Taiwan”. *Taiwan Strategists, 2*. https://www.pf.org.tw/files/6510/A73CE07D-0D72-4AF8-9075-98A1CB188DA1
28. Smagh, N. S. (4 June 2020). “Intelligence, surveillance and reconnaissance design for great power competition”. *Congressional Research Service*. https://news.usni.org/2020/06/07/report-to-congress-on-intelligence-surveillance-and-reconnaissance-for-great-power-competition
29. The White House. (2021). *The Interim National Security Strategic Guidance.* https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf
30. The World Bank. (2021). *The world bank in China.* https://www.worldbank.org/en/country/china/overview
31. Tjan, Sie Tek (25 September 2020). "SAFE releases China's net International Investment Position (NIIP) as of the end of June 2020". www.safe.gov.cn.
32. Tkacik, M. (2018). “Understanding China’s and strategy in the South China Sea: bringing context to a revisionist systemic challenge – intentions and impact” *Defense & Security Analysis, 34* (4), pp. 321-344. https://doi.org/10.1080/14751798.2018.1529092
33. Winkels, J. (2017). “Expanding integrated coalition and NGO ISR to better support HA/DR Operations”. *American Intelligence Journal, 34*(1), pp. 97-101. https://www.jstor.org/stable/26497123