Competing in the Ether:
Countering PRC Gray Zone Operations with a South China Sea Cyberspace Coalition

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
13-05-2022	FINAL	N/A

4. TITLE AND SUBTITLE

Competing in the Ether: Countering PRC Gray Zone Operations with a South China Sea Cyberspace Coalition

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Craig T. McLemore

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Writing & Teaching Excellence Center
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

As targets of Chinese Gray Zone influence operations, the nations of the South China Sea (SCS) region are fertile ground for USINDOPACOM to plant seeds of cooperation (and perhaps future coalition) in opposition to the CPC. The growing influence of Information Technology (IT) and cyberspace in military operations (particularly Chinese Gray Zone operations) present unique opportunities for cooperation. USINDOPACOM can bolster the security of US national interests within the SCS region by opposing Chinese Gray Zone operations against their neighbors.

15. SUBJECT TERMS (Key words)
Space, Coalition, Multinational Force, Space Strategy, Outer Space Treaty, UNOOSA

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	N/A	19	Director, Writing Center
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			19b. TELEPHONE NUMBER *(include area code)* 401-841-6499

Competing in the Ether

1. Introduction and Thesis

Over the summer of 2021, the Communist Party of China (CPC) declared that the People's Republic of China (PRC) had become a "moderately prosperous society in all respects," achieving a major goal set in 1982.[1] Though the PRC has made significant progress in achieving modernization and affluence, the CPC aims toward a significantly greater impact on the world stage. By exercising soft power and threatening the use of hard power (Gray Zone tactics), the CPC seeks to establish dominance of East Asia and to diminish American influence around the globe. As the Unified Combatant Command (UCC) responsible for South and East Asia, United States Indo-Pacific Command (USINDOPACOM) must meet China in the Gray Zone to secure US interests within their Area of Responsibility (AOR).

As targets of Chinese Gray Zone influence operations, the nations of the South China Sea (SCS) region are fertile ground for USINDOPACOM to plant seeds of cooperation (and perhaps future coalition) in opposition to the CPC. The growing influence of Information Technology (IT) and cyberspace in military operations (particularly Chinese Gray Zone operations) present unique opportunities for cooperation. USINDOPACOM can bolster the security of US national interests within the SCS region by opposing Chinese Gray Zone operations against their neighbors. To this end, the USINDOPACOM Commander must establish cyberspace and IT partnerships with SCS regional nations under the auspices of the South China Sea Initiative (SCSI)[2] to diminish China's ability to influence its neighbors through Gray Zone operations. To build this SCS coalition against PRC Gray Zone activities, the USINDOPACOM Commander must explicate to regional nations the information, economic, and military risks of cooperating

[1] "China Focus: Xi declares China a moderately prosperous society in all respects," *Xinhua*, July 1, 2021. http://www.xinhuanet.com/english/special/2021-07/01/c_1310038553.htm
[2] *South China Sea Initiative*, 10 USC § 2282 (2016), 129 STAT 1073-1075. https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf

with or capitulating to China, as well as presenting cooperation with the U.S. as a beneficial alternative in those same areas.

2. Background

The American military is most comfortable operating in the clearly defined spaces of war and peace: either conducting armed conflict or not. In the liminal space between the two, however, lies a broad area of national competition known as the Gray Zone. Military actions in this space are designed to stay below the threshold of provoking lethal conflict through gradual erosion of the status quo and without threatening the existential or vital interests of one's competitor.[3] Further, actors in the Gray Zone attempt to avoid attribution, or else extensively justify their actions legally and politically.[4] The PRC employs a wide variety of Gray Zone activities to bolster its expansionist claims in the SCS, notably economic coercion, cyberspace operations, and influence operations.[5]

The BRI is a comprehensive program of economic cooperation between China and numerous Eurasian countries. This conglomeration of projects proposes to build land and maritime trade routes, energy corridors, and infrastructure from China to Indochina, the Indian subcontinent, Russia, Africa, and western Europe.[6] One important but underrated component of this program (outside of China) is investment in IT infrastructure in underdeveloped countries.

[3] Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, (2019), Rand Report. www.rand.org/t/RR2942, pp. 8-10
[4] Ibid.
[5] Morris et al., "Competitive Advantage" 27-36
[6] "China's 'One Belt, One Road' Initiative: An ESCAP Report." *Population and Development Review* 43, no. 3 (2017): 583–87. http://www.jstor.org/stable/26622845.

Inside of China, however, leadership in both the private and public sectors recognizes the criticality of communications infrastructure to bolstering the PRC's prestige and influence.[7]

Based on a proposed Senate Bill, the Asia-Pacific Maritime Security Initiative of 2016,[8] the SCSI is a provision of the 2016 NDAA. SCSI allows the cognizant UCC (under the auspices of the Secretary of Defense) to conduct maritime Theater Security Cooperation (TSC) in furtherance of a stable and peaceful SCS.[9] Noteworthy for the context of this paper, the SCSI specifies only the maritime domain and maritime operations as venues for TSC.

3. Information

To oppose Chinese encroachment and influence in the information domain, USINDOPACOM must seek cooperation and partnership with nations in the SCS region. In pursuit of this end, UNSINDOPACOM must first convince those nations of the informational risk induced by accepting Chinese assistance in building their infrastructure under the BRI. Doing so will require a multilayered case showing China as a malicious actor within the information domain. USINDOPACOM must demonstrate that Chinese firms working abroad generally act as pawns of the CPC. Additionally, USINDOPACOM must convince SCS regional stakeholders that China habitually uses cyber operations as a means of imposing their will or weakening the will of opposing nations. These facts together mean that adoption of Chinese IT necessarily weakens a nation's position in a real-world confrontation with the PRC.

[7] Hong Shen, "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative," *International Journal of Communication* 12 (2018): 2683–2701. https://ijoc.org/index.php/ijoc/article/view/8405
[8] Asia-Pacific Maritime Security Initiative Act of 2016, S. 2685, 114th Congress, (2016). https://www.congress.gov/bill/114th-congress/senate-bill/2865/text
[9] SCSI, 129 STAT 1073-1074

More than almost any other country, the PRC operates a vast number of State-Owned Enterprises (SOEs), including several major IT, electronics, and telecommunications firms.[10] The CPC routinely uses these SOEs as instruments of national policy within the SCS region (particularly through infrastructure development).[11] In addition to SOEs, the CPC exercises a significant amount of control over companies with headquarters in the PRC. Troublingly, the Xi-era trend toward tighter integration between the party and both SOEs and private sector companies appears unlikely to change (and likely to increase).[12] As such, Chinese technology companies (SOE or private) building infrastructure for SCS nations under the BRI either directly or indirectly assist the CPC's vision of continually growing national prosperity.[13] In light of those nations' competing claims over maritime territory, we can conclude that the PRC will attempt to use the BRI as a means of influencing concessions (or at least tolerance) from SCS nations with whom they have territorial disputes. The PRC, however, does not constrain itself to exercising only such soft power as the BRI to achieve its national ends.

As a nation capable of extensive and sustained cyber operations, China employs both positive (enticing) and negative (coercive) cyber operations as means of the Information instrument of national power.[14] By doing so, China enjoys many of the same benefits that they would through the diplomatic and military instruments: enticement to find a mutually acceptable solution to a dispute, or else holding at risk some critical component of a nation's infrastructure or economy to force capitulation. The PRC habitually and increasingly uses cyber and influence

[10] State Council, *Directory*, State Owned Assets Supervision and Administration Commission, (June 29, 2021). http://en.sasac.gov.cn/directorynames.html
[11] Gong, Xue, "The Role of Chinese Corporate Players in China's South China Sea Policy," *Contemporary Southeast Asia* 40, No. 2 (2018): 314-317. DOI: 10.1355/cs40-2f
[12] Zhang, Xianchu, "Integration of CCP Leadership with Corporate Governance: Leading Role or Dismemberment?" *China Perspectives* 2019, no. 1, (2019): 55-63. https://www.proquest.com/docview/2199061765
[13] Shen, "Digital Silk Road," 2686-2688.
[14] Brandon Valeriano, Benjamin Jensen, and Ryan C Maness. "Cyber Coercion as a Combined Strategy" in *Cyber Strategy: the Evolving Character of Power and Coercion*, (New York: Oxford University Press, 2018), 89-109.

operations as part of its Gray Zone repertoire to either bully weaker nations or push back stronger ones without prompting a military response.[15] Internationally, the government of the PRC has been shown to employ a wide variety of tactics in cyberspace, including extracting information on foreign governments' internal functions, embedding backdoors in networking devices for later exploitation, or conducting direct attacks via BotNets or other methodologies.[16] In the SCS specifically, the PRC employs influence and cyber as means to respectively bolster its maritime claims on the international stage (especially through propaganda) or to coerce its neighbors to capitulate to its expansionist claims in that region (through offensive cyber operations).[17] As a major power in cyberspace, China can exercise significant capability to entice or coerce concessions from virtually any nation in the world. This principle is particularly true of those nations with both increasing penetration of IT in daily life and significant vulnerabilities in cyberspace.

The employment of SOEs and private sector companies as arms of the CPC abroad doesn't mean that their IT, communications, and electronics equipment categorically introduce vulnerabilities into other nations' infrastructures. It would be foolhardy, however, to presume that the People's Liberation Army (PLA) will not seek to use such equipment to their benefit. The PRC's employment of Gray Zone cyber operations as means of political coercion makes the Information risk of accepting Chinese communications infrastructure especially poignant. Chinese IT, communications, and electronics firms know their equipment and software better than any third party can, if for no other reason than because they manufacture it. When Chinese

[15] Mark Bryan Mantanan, "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, September 2020, 1-29. DOI: 10.1142/S1013251120400135
[16] Center for Strategic and International Studies, Significant Cyber Incidents Since 2006, September 2021. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[17] Morris et al., "Competitive Advantage," 35-36

firms build IT infrastructure in SCS nations under the auspices of the BRI, they introduce potential attack vectors (whether intentionally or unintentionally) for PLA cyber operators to exploit. USINDOPACOM must make the case that the Information risk of voluntarily allowing the PRC a potential attack vector for coercive cyber operations is too high. The risk of such operations, however, extends beyond pure Information considerations, and into the Economic; accordingly, so must USINDOPACOM's argument to SCS nations.

4. Economy

Having established the PRC's Information threat to the sovereignty of SCS nations, USINDOPACOM must next demonstrate that the costs of Chinese infrastructural assistance outweigh any perceived benefits. The governments of SCS nations must first recognize that the BRI is not designed to facilitate their national well-being in the long run; it instead makes them beholden to Chinese interests in general and (indirectly) to the CPC specifically. SCS governments must also understand the long term Economic risk of information exploitation and exfiltration by malicious actors. USINDOPACOM must finally present an economically viable and palatable alternative to Chinese infrastructure. By establishing the economic case against cooperating with China and presenting alternatives to SCS nations, USINDOPACOM will bolster the case for cooperating with the US in opposition to the PRC.

Despite any economic benefits to the nations who accept BRI investment, the system is fundamentally designed to influence (or control) participant nations to the benefit of the PRC. The Digital Silk Road (DSR), the IT component of the BRI, encompasses the infrastructural practices discussed previously, in addition to several others designed to increase the PRC's power and influence abroad. Among these DSR initiatives are the gradual recentering of global

communication networks on China (building PRC cyberspace advantage); finding export markets for China's excess productive capacity (foreign currency surplus); and the internationalization of the Renminbi (competing with the USD as international reserve currency).[18] By the combination of these and other practices included under the penumbra of the BRI, the PRC is attempting to construct an alternate world order centered on the interests of the PRC and the CPC. The CPC's desire to establish PRC regional hegemony necessitates SCS nations as immediate targets for Beijing's strategy of political influence through economic investment.[19] But the PRC does not historically limit its economic activities in the information domain to investment and trade; SCS nations must also beware of economic extraction by means of data exfiltration – particularly intellectual property.

In recent years, the impacts of cyber attacks on businesses, academic institutions, and even individual users have received increasing media attention. Though identifying the perpetrators of cyber attacks is notoriously difficult, cybersecurity consulting firm Mandiant attributes 29 distinct Advanced Persistent Threat (APT) groups to China, including a named PLA formation (the infamous Unit 61398).[20] Using a wide variety of tactics (from simple phishing to advanced zero-day exploits), these groups attack public and private sector actors around the world to gain sensitive political, technical, and economic information.[21] This information can then provide intelligence support to the CPC and PLA or allow Chinese companies competitive advantages against foreign companies. Based on post-attack and trend analysis, one might reasonably reach two major conclusions: Chinese APT groups conduct economic espionage on behalf of interests within the PRC, and this method of economic warfare by PLA actors will only

[18] Shen, "Building a DSR," 2686-2692.
[19] Derived from "ESCAP Report," 583-584, and Shen, "Building a DSR," 2686-2692
[20] Mandiant, Advanced Persistent Threat Groups, (n.d.). https://www.mandiant.com/resources/apt-groups
[21] Ibid.

grow in frequency and intensity.[22] Recalling the close cooperation between Chinese technology companies and the CPC (potentially acting as arms of the CPC through the BRI), it is decidedly against the economic interests of SCS nations to allow Chinese IT within their critical infrastructure. To do so is to willingly introduce a major attack surface for malicious PRC cyber actors (whether PLA or partisan) to exploit. If even a firm as technologically savvy as Google has proven susceptible to these groups' efforts,[23] and the international financial community fears critical organizational reforms due to the threat from APTs,[24] then SCS nations should not outsource their IT infrastructure to Chinese firms.

Having established the economic dangers of the BRI, USINDOPACOM must make the case that cooperation with the US is a palatable alternative. While the disconnect between US Government and US companies should comfort SCS nations with respect to cybersecurity risk (and risk of economic extraction), the difference in cost between Chinese and American technology will be a sticking point. USINDOPACOM should seek a whole-of-government approach (DoS-coordinated cooperative lending with allies, loans through US Export-Import Bank, etc.) to assist potential SCS partners in building IT independence from China.[25] Additionally (or alternatively), USINDOPACOM should seek to build a coalition among SCS nations or work with existing institutions to build a framework for regional cooperation on IT

[22] Ainikki Riikonen, "Decide, Disrupt, Destroy: Information Systems in Great Power Competition with China," Strategic Studies Quarterly 13, no. 4, 122-145. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_proquest_reports_2393081223

[23] Ellen Messmer, "Google hack malware said to be Chinese in origin; Researcher finds clues in Trojan code of Operation Aurora," *Network World*, January 20, 2010. https://advance-lexis-com.usnwc.idm.oclc.org/api/document?collection=news&id=urn:contentItem:7XMN-JD40-Y9NM-51XW-00000-00&context=1516831.

[24] Microsoft Corporation, "Fear of Cyberattacks Impedes Progress of Digital Transformation in Financial Services Companies in APAC." Networks Asia [trade journal] (Nov 20, 2018).

[25] Malanie Hart and Jordan Link, There Is a Solution to the Huawei Challenge, Center for American Progress Foreign Policy and Security Report, October 14, 2020. https://www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge/

infrastructure. More important than helping finance or organize the effort, though, USINDOPACOM must stress that the priority is to get China out of SCS nations' infrastructure, regardless of where the ultimate parts suppliers are headquartered; pushing American products while decrying China's bullishness will not win partners. By demonstrating America's good faith and concern for SCS nations' independence, USINDOPACOM might present an economically palatable alternative to the BRI. Even with assistance in building an IT infrastructure independent of China, however, SCS nations will need some level of US security cooperation in cyberspace to mitigate the Chinese military threat.

5. Military

Once SCS nations understand that the information and economic risks of accepting Chinese investment through the BRI outweigh the benefits (and that there are reasonable alternatives), USINDOPACOM must entice them to cooperate with the US military and our mission partners. The commander must underscore to potential partner nations the military threat posed by PRC (and especially PLA) cyber activities. The commander can then make the case for US military personnel to provide network defense consultation and training in addition to testing of both network defense personnel and the defenses themselves to better secure partner nations' IT infrastructure. Finally, working toward collaboration (and possibly coalition) with SCS nations in cyberspace will necessitate a shift in US policy; USINDOPACOM Commander must advocate additional language for the SCSI adding regional cooperation on IT and cyber operations as priorities for his command.

The PLA exploits its cyberspace capabilities to gain military advantages in the physical domains of warfare. Some APTs conduct general operations against groups and nations the CPC

perceives as threats or hindrances to party ambitions; APTs 23 and 30, for instance, specifically target ASEAN or some subset thereof.[26] Other suspected PLA APTs (e.g. 7, 15, 26, and 31), confine their operations to the extraction of intellectual property in defense-sensitive sectors, such as aerospace, energy, high technology, telecommunications, and transportation.[27] Still other groups have very narrow mission sets, targeting specific strategic advantages that the PLA desires to achieve. APT40 narrowly targets nations party to SCS maritime disputes with the PRC and nations possessing significant naval technology, suggesting a mission of facilitating PRC maritime superiority in the SCS.[28] Regardless the alignment of the group (geographic, public/private sector, or specific mission), PLA Offensive Cyber Operations (OCO) pose a significant threat to SCS nations. While some nations in the region (e.g. Vietnam) have exhibited noteworthy capabilities in cyberspace,[29] others need assistance in building their Defensive Cyber Operations (DCO).[30] As the cognizant UCC for a preeminent cyberspace power, USINDOPACOM is well positioned to render such assistance.

Like most nations with robust cyberspace capabilities, the US hesitates to cooperate with any nations but the closest of allies in cyber operations. Unlike more traditional materiel and methods of war, a single use of an OCO capability or tactic can render it obsolete by alerting the world to its existence. Like any other martial discipline, developing military expertise in cyberspace operations is at least as important acquiring tools, and especially so in the SCS

[26] Mandiant, *APT Groups*
[27] Ibid.
[28] Riikonen, "Decide, Disrupt, Destroy," 128.
Riikonen asserts their mission to be facilitating the building of a blue-water Navy. Based on the purpose of this paper and the evidence cited, I assert a mission of facilitating local dominance of the SCS – a difference in scale, but not in purpose
[29] CSIS, *Significant Cyber Incidents*
[30] Caitriona H. Heinl, *Enabling Better Multinational and International Military Cooperation for Cyber-related Matters across Asia and Europe*, Rajaratnam School of International Studies Centre of Excellence for National Security Policy Report, (2015). https://www.jstor.org/stable/resrep05877

region.[31] There is significant collaboration already (such as through NATO) in sharing expertise and lessons learned, consultation on defensive best practices, and other such DCO activities.[32] Similarly, the Exercise CROSSED SWORDS 2019 demonstrated that OCO simulation within a multinational context is not only possible, but desirable.[33] As such, there is precedent for USINDOPACOM (in collaboration with US Cyber Command) to allocate both DCO and (simulated) OCO forces in support of TSC operations with putative mission partners in the SCS region. With additional experience, USINDOPACOM could consider incorporating robust cyber presentations into existing international exercises involving SCS partners like RIMPAC and TALISMAN SABRE. To execute such an aggressive plan of action, however, USINDOPACOM must first address policy concerns at home.

The proposition of cooperation with nontraditional coalition partners in a sensitive area like cyber operations will doubtless face stiff resistance in Washington. With good reason, the military establishment and lawmakers desire to keep a close hold on national capabilities like OCO. Regardless, USINDOPACOM must make the case for modifying the SCSI to formalize US support to SCS nations in cyberspace. President Biden considers both cooperation with partner nations and curbing destabilizing activities in cyberspace high priorities for the Defense establishment.[34] He further holds that stronger relationships with SCS nations are critical to US national interests in the Indo-Pacific region.[35] Considering the PRC's proclivity for bullying its

[31] Heinl, *Enabling Better Cooperation for Cyber*
[32] Muzaffer Satiroglu, *Cyber Interoperability and Cooperation: Why are States Reluctant?*. Reading: Academic Conferences International Limited, 2018. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_proquest_journals_2077000314
[33] Bernhards Blumbergs, Rain Ottis, and Risto Vaarandi. Crossed Swords: A Cyber Red Team Oriented Technical Exercise. Reading: Academic Conferences International Limited, 2019. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_proquest_journals_2261016935
[34] *Interim National Security Strategic Guidance*, (March 3, 2021). https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf
[35] Ibid.

neighbors in cyberspace and ability to do far worse, USINDOPACOM must collaborate with SCS nations to strengthen their cybersecurity posture. The President's clear intent necessitates that the USINDOPACOM commander advocate Congressional modification of the SCSI to account for the cyber domain – not just the maritime – as a venue for collaboration and security cooperation in the SCS region. Cyberspace materiel, advice, training, and exercises are critical requirements for USINDOPACOM to counter the PRC in the Gray Zone in furtherance of a more stable and peaceful Indo-Pacific.

6. Counterargument

Despite the potential benefits, a coalition to counter PRC Gray Zone operations in cyberspace might not be in the cards. Holmes and Yoshihara state the case against coalition succinctly: "This region tends toward political entropy."[36] Competing claims in the SCS and divergent political goals might doom regional coalition from the outset. Allied action to counter China might instead focus on Northeast Asia due to political stability, proximity of reliable allies, and the smaller scale of contested areas.[37] The fundamentally geographic nature of the seemingly intractable SCS dispute lends some credence to this approach. How is the US to bring together so many nations with such fundamental political disagreements fast enough to be meaningful in the competition with the PRC?

Rather than seeking the "big win" in the SCS today, pivot instead to a less contested area with existing allies who have robust cyber operations capabilities. Japan and Korea are both top ten nations in cybersecurity, with perfect or near-perfect scores in all areas measured (legal,

[36] James R. Holmes, and Toshi Yoshihara, "Deterring China in the 'Gray Zone': Lessons of the South China Sea for U.S. Alliances," *Orbis* 61, no. 3 (2017): 336. https://doi.org/10.1016/j.orbis.2017.05.002
[37] Ibid.

technical, organizational, capacity, and cooperation).[38] Notwithstanding the historical enmity between Japan and Korea, the US can help to ease tensions between them and encourage trilateral cooperation on pressing issues like cybersecurity.[39] USINDOPACOM's limited resources might be better spent seeking a "quick win" in Northeast Asia as an external staging point for long-term SCS Gray Zone Competition.[40] The smaller area of contested waterspace, high technological savvy of the potential partners, and pre-existing bilateral security agreements in Northeast Asia make the prospect attractive.

7. Rebuttal

Gray Zone operations are necessary to counter Gray Zone operations. Due to expense and difficulty of execution Freedom of Navigation exercises can only happen so often, and public condemnation of China's aggressive policy toward their SCS neighbors can only accomplish limited impact. Asymmetric means of military confrontation (e.g. bilateral and multilateral agreements) would send a tangible message to the CPC that the US means to counter their expansionism in the SCS.[41] In the long-term Gray Zone competition with China, multilateral confrontation will be a critical asset to achieving US ends.[42] While a trilateral agreement with Japan and Korea would be a significant achievement in countering China's claims in the East

[38] International Telecommunications Union, *Global Cybersecurity Index* 2020, https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/
[39] Kathryn Botto, *Overcoming Obstacles to Trilateral U.S.-ROK-Japan Interoperability*, Carnegie Endowment Report, March 18, 2020. https://carnegieendowment.org/2020/03/18/ overcoming-obstacles-to-trilateral-u.s.-rok-japan-interoperability-pub-81236
[40] Holmes and Yoshihara
[41] Michael O'Hanlon, *China, the Gray Zone, and Contingency Planning at the Department of Defense and Beyond*, Brookings Institution Report, September 2019. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_proquest_reports_2577501177
[42] Rand, *Gaining Competitive Advantage*, 131-132.

China Sea, it would do little (if anything at all) to address the fast-paced, high-stakes contest in the SCS.

The US must confront China where China is, not just operationally, but geographically as well. In a recent article, Holmes argues that permanent US presence in the SCS is critical to successfully countering their Gray Zone tactics there.[43] Unlike operations with traditional military hardware, cyberspace cooperation or coalition in the SCS would be a relatively low-investment, perpetual presence proposition. While multilateral cyberspace cooperation in the region might not be feasible in the near term, a series of bilateral agreements might be. From that point, USINDOPACOM (in coordination with DoS) can work toward a comprehensive, multilateral SCS cybersecurity agreement. The high-intensity contest is in the SCS; failure to contest excessive PRC claims there is tantamount to assent.

8. Conclusion

USINDOPACOM must counter PRC Gray Zone cyber operations in the SCS by building a coalition of SCS states oriented toward matching the PRC in the Gray Zone. To build this coalition, the USINDOPACOM commander must first articulate the Information threat of the BRI by showing Chinese IT firms to be malicious actors and making the case that accepting their equipment would necessarily undermine the security of SCS nations. He must next prove that the Economic cost of the BRI would too dear in terms of loss of autonomy and economic extraction, while cooperation with the US presents an acceptable alternative. Third, he must evoke the Military threat of PLA cyber operations against SCS nations, while offering to assist them in building their own defenses. Finally, Congress must change the SCSI to formally authorize SCS

[43] James R., Holmes, "To Beat China In The Gray Zone, You Have To Be There," 1945, July 28, 2021. https://www.19fortyfive.com/2021/07/to-beat-china-in-the-gray-zone-you-have-to-be-there/

cyberspace coalition-building and TSC activities undertaken by USINDOPACOM. The US must counter China in the SCS now, and cyberspace is the logical place to do it.

Bibliography

Asia-Pacific Maritime Security Initiative Act of 2016, S. 2685, 114th Congress, (2016). https://www.congress.gov/bill/114th-congress/senate-bill/2865/text

Blumbergs, Bernhards, Rain Ottis, and Risto Vaarandi. *Crossed Swords: A Cyber Red Team Oriented Technical Exercise.* Reading: Academic Conferences International Limited, 2019. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_proquest_journals_2261016935

Botto, Kathryn, *Overcoming Obstacles to Trilateral U.S.-ROK-Japan Interoperability*, Carnegie Endowment Report, March 18, 2020. https://carnegieendowment.org/2020/03/18/overcoming-obstacles-to-trilateral-u.s.-rok-japan-interoperability-pub-81236

Center for Strategic and International Studies, *Significant Cyber Incidents Since 2006*, September 2021. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

"China Focus: Xi declares China a moderately prosperous society in all respects," *Xinhua*, July 1, 2021. http://www.xinhuanet.com/english/special/2021-07/01/c_1310038553.htm

"China's 'One Belt, One Road' Initiative: An ESCAP Report." *Population and Development Review* 43, no. 3 (2017): 583–87. http://www.jstor.org/stable/26622845.

Gong, Xue, "The Role of Chinese Corporate Players in China's South China Sea Policy," *Contemporary Southeast Asia* 40, No. 2 (2018): 301-326. DOI: 10.1355/cs40-2f

Hart, Malanie, and Jordan Link, *There Is a Solution to the Huawei Challenge, Center for American Progress Foreign Policy and Security Report*, October 14, 2020. https://www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge/

Heinl, Caitriona H., *Enabling Better Multinational and International Military Cooperation for Cyber-related Matters across Asia and Europe*, Rajaratnam School of International Studies Centre of Excellence for National Security Policy Report, (2015). https://www.jstor.org/stable/resrep05877

Holmes, James R., "To Beat China In The Gray Zone, You Have To Be There," *1945*, July 28, 2021. https://www.19fortyfive.com/2021/07/to-beat-china-in-the-gray-zone-you-have-to-be-there/

Holmes, James R., and Toshi Yoshihara, "Deterring China in the 'Gray Zone': Lessons of the South China Sea for U.S. Alliances," *Orbis* 61, no. 3 (2017): 322-339. https://doi.org/10.1016/j.orbis.2017.05.002

Interim National Security Strategic Guidance, (March 3, 2021). https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

Mandiant, *Advanced Persistent Threat Groups*, (n.d.). https://www.mandiant.com/resources/apt-groups

Mantanan, Mark Bryan, "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, September 2020, 1-29. DOI: 10.1142/S1013251120400135

Messmer, Ellen, "Google hack malware said to be Chinese in origin; Researcher finds clues in Trojan code of Operation Aurora," *Network World*, January 20, 2010. https://advance-lexis-com.usnwc.idm.oclc.org/api/document?collection=news&id=urn:contentItem:7XMN-JD40-Y9NM-51XW-00000-00&context=1516831.

Microsoft Corporation, "Fear of Cyberattacks Impedes Progress of Digital Transformation in Financial Services Companies in APAC." *Networks Asia* [trade journal] (Nov 20, 2018).

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Keep, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, (2019), Rand Report. www.rand.org/t/RR2942

O'Hanlon, Michael, *China, the Gray Zone, and Contingency Planning at the Department of Defense and Beyond*, Brookings Institution Report, September 2019. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_proquest_reports_2577501177

Riikonen, Ainikki, "Decide, Disrupt, Destroy: Information Systems in Great Power Competition with China," *Strategic Studies Quarterly* 13, no. 4, 122-145. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_proquest_reports_2393081223 128

Satiroglu, Muzaffer, *Cyber Interoperability and Cooperation: Why are States Reluctant?*, Reading: Academic Conferences International Limited, 2018. https://usnwc.primo.exlibrisgroup.com/permalink/01USNWC_INST/ouaji3/cdi_proquest_journals_2077000314

Shen, Hong, "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative," *International Journal of Communication* 2018, no. 12, 2683–2701. https://ijoc.org/index.php/ijoc/article/view/8405

South China Sea Initiative, 10 USC § 2282 (2016). https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf

State Council, *Directory*, State Owned Assets Supervision and Administration Commission, (June 29, 2021). http://en.sasac.gov.cn/directorynames.html

Valeriano, Brandon, Benjamin Jensen, and Ryan C Maness. "Cyber Coercion as a Combined Strategy" in *Cyber Strategy: the Evolving Character of Power and Coercion*, (New York: Oxford University Press, 2018), 89-109.

Zhang, Xianchu, "Integration of CCP Leadership with Corporate Governance: Leading Role or Dismemberment?" China perspectives 2019, no. 1, (2019): 55-63. https://www.proquest.com/docview/2199061765

Appendix: Glossary of Terms

AOR – Area of Responsibility

BRI – Belt and Road Initiative

CPC – Communist Party of China

DCO – Defensive Cyber Operations

DSR – Digital Silk Road

IT – Information Technology

OCO – Offensive Cyber Operations

PLA – People's Liberation Army

PRC – People's Republic of China

SCS – South China Sea

SCSI – South China Sea Initiative (section 2282 of the 2016 NDAA)

SOE – State-Owned Enterprise

TSC – Theater Security Cooperation

UCC – Unified Combatant Command

USINDOPACOM – United States Indo-Pacific Command