ZULFAQAR Journal of
Defence Management, Social Science & Humanities

Journal homepage: https://zulfaqarjdmssh.upnm.edu.my/index.php/zjdmssh

HOW CHINA USE CYBER NETWORKS WITH DRONES TO MONITOR THE SPRATLY ISLANDS IN THE SOUTH CHINA SEA

Nur Sabrina Mohamad Sharif[a,*], **Adam Leong Kok Wey**[b]

[ab] National Defence University of Malaysia, Kem Sungai Besi, 57000, Kuala Lumpur

*Corresponding author: sabrinasharif7@gmail.com

ARTICLE INFO

Article history:
Received
30-09-2022
Received in revised
17-04-2023
Accepted
19-04-2023
Available online
30-06-2023

Keywords:
China, cyber power, drones, technology

e-ISSN: 2773-529X
Type: Article

ABSTRACT

The South China Sea disputes are mainly related to delimitations concerning islands and reefs in the South China Sea and adjoining waters. The claimant states are China, Vietnam, the Philippines, Malaysia, and Brunei. Claimants' states are keen on holding or gaining the freedom to fish stocks, the investigation and expected abuse of unrefined petroleum and flammable gas in the seabed of different areas of the South China Sea, and the essential control of significant delivery paths. The Spratly Islands issue can be assessed from an assortment of points. Regarding public safety, these islands are significant because of their locations in the South China Sea, where numerous merchant ships carry merchandise, individuals, and energy to Asian-Pacific nations. Drones, as sophisticated tools connected and controlled by cyber technology, are used to observe the conditions of the islands from long distances. The methodology used in this article is the qualitative method. The data was collected from a variety of articles that related to this topic. This article analyses how effectively China uses drones with cyber power to monitor the Spratly Islands. This article focuses more on the operational, tactical, and strategic advantages of drone monitoring of Spratly Island in the South China Sea.

DOI: *http://doi.org/10.58247/jdmssh-2023-0601-04*

INTRODUCTION

Background of South China Sea

Cyberpower is a society's organised capability to leverage digital technology for surveillance, exploitation, subversion, and coercion in international conflict. A society with significant cyber power can economically exploit or undermine other nations; gather political and military intelligence more efficiently than pre-digital espionage; interfere in foreign political discourse online; degrade an adversary's warfighting capabilities; sabotage critical infrastructure and industrial mass production; and even cause mass casualties. All of this is possible with the intelligent application of digital technology without the need for military forces or human spies.

The South China Sea extends from the Strait of Malacca in the southwest to the Strait of Taiwan in the northeast. Over 500 million people in China, Taiwan and the ASEAN countries, the Philippines, Malaysia, Brunei, Indonesia, Singapore, Cambodia, Thailand, and Vietnam, live within 100 miles of their coastline. It has remarkable biological diversity, including over 30% of the world's coral reefs and many

valuable fisheries (Hayton, 2014). It is also thought to contain abundant oil and natural gas, a prospect of vital interest to energy-importing countries.

It is one of the world's busiest global ocean paths, with many of its busiest delivery ports. Each year, over a portion of the world's significant oil haulier traffic and a portion of the world's dealer armada sail through its waters. It is a vital sea connection between the Pacific Ocean and the Indian Ocean, and along these lines, it is of principal significance to major maritime forces. The South China Sea is a growing concern over conflicting territorial claims, piracy, poaching, resource depletion, pollution, drug trafficking, illegal migration, and the threat of terrorism.

Spratly Islands

The Spratly Islands are a large group of reefs, shoals, atolls, and small islets in the South China Sea of the Pacific Ocean. They are located north of insular Malaysia and are roughly midway between Vietnam and the Philippines, and they are claimed wholly or in part by several countries in the region. The Spratlys are spread out over a vast area of ocean measuring some 158,000 square miles. A significant number of them are submerged. Spratly Island or Storm Island, measuring 900 to 1,500 feet, is uninhabited by humans and supports only turtles and seabirds as wildlife (Hayton, 2014).

By the late twentieth century, Vietnam, China, Taiwan, and Malaysia had control of the Terumbu Layang-Layang reef in June 1983, and the Philippines had all had clashing cases with the Spratlys, which were supported by a post on various islands (Chang, 1991). Although Brunei did not guarantee any region in the Spratlys, it declared an Exclusive Economic Zone (EEZ) that contained a Spratly reef. The United States, which has been the dominant presence in the Pacific region since the early 20th century, has not recognised any country's claims on the Spratlys, insisting instead that the Spratlys are in international waters. China has stated that its case against the Spratlys goes back hundreds of years. The Chinese government has expressed that the South China Sea, including the Spratlys and other island gatherings, is within its effective reach. Those cases have been firmly questioned by the Philippines and Vietnam specifically. China previously settled a dispute in the Spratlys in 1988, when its military persuasively eliminated a Vietnamese post from Johnson South Reef. In mid-2014, China started developing counterfeit land on specific reefs and atolls. That action and China's more grounded articulations on its asserted regional uprightness in the Spratlys heightened tensions with the U.S. which dispatched a U.S. warship through the district in October 2015 (Loja, 2016).

The Importance of the South China Sea

As China consolidates its position in the Spratly Islands, piling sand and constructing airstrips on the contentious reefs in the middle of the South China Sea, the world's attention has returned to the region's long-standing territorial disputes. While naval plans and more significant military doctrine have dominated recent headlines, one critical element of modern combat has been notably absent from the South China Sea debate: cyberspace. If history is any indicator, future escalation in the disputed waters will almost certainly cross over into the cyber world, regardless of where it begins. According to FireEye, Kaspersky Lab's Securelist, and CrowdStrike findings, the Southeast Asian claims to the South China Sea, together with private companies doing business in the region, have been common targets of advanced infiltration operations launched from China. Chinese cyber units and malware versions have infiltrated regional public networks, primarily targeting top-level government entities and civil and military organisations in the Philippines and Vietnam (Diplomat, 2015).

China's cyber actions are a means to an end in the real world, and they can potentially escalate simmering tensions into a full-fledged fight, both online and offline. Beijing has exploited its cyber capabilities to support other, often hazardous diplomatic manoeuvres. Indeed, during heightened tensions, the number of cyberattacks has increased dramatically, with China attempting to obtain vital security information to gain a strategic advantage over its regional rivals. For instance, in May 2014, China moved an oil rig into Vietnamese waters, causing an international issue. Both countries' vessels participated in water-cannon fights, and fatal anti-China protests erupted in Vietnam. China expanded the warfare beyond land and sea, attacking the Vietnamese government and military entities with spear-phishing attacks that distributed malware-infected papers. The threat actors most likely breached a Vietnamese intelligence agency's network, obtaining access to vital information concerning the country's security strategy (Gonzales, 2014).

In October 2014, there was a noticeable increase in cyber-attacks from China targeting Vietnamese networks, probably due to Vietnamese weaponry purchases aimed at improving its marine security capabilities. As a result of these instances, Vietnam named the most targeted country in cyberspace in 2014. Vietnam is not the only South China Sea claimant targeted by Chinese hacking. Chinese patrol warships docked in waters near the Philippine-claimed Scarborough Shoal in April 2012. The Philippines was obliged to withdraw its ships after a heated confrontation. Simultaneously, hackers from both sides launched massive defacement efforts against the government, media, and academic websites. A Chinese cyber squad successfully infiltrated the Philippine government and military networks, seizing military records, internal conversations, and other sensitive dispute materials (Gonzales, 2014).

With China's island-building spree picking up steam and the preliminary verdict of the arbitral tribunal in the Philippines' legal challenge against China expected by the end of the year, tensions in the South China Sea will remain high. Furthermore, as previous clashes in the region have demonstrated, problems in the actual world will surely spill over online. Strong cyber defences are critical for a country's capacity to protect sensitive national security information and keep many of its vital activities operational (Diplomat, 2015). However, Vietnam, the Philippines, and other Association of Southeast Asian Nations (ASEAN) states bordering the South China Sea have inadequate cyber capabilities. If tensions rise into an open conflict and the attacks progress from cyber espionage and relatively innocuous website defacement to causing significant damage to crucial infrastructure or government networks, ASEAN countries would have virtually no method of halting them. Moreover, despite its geographical distance, if the United States were removed from the territorial disputes, its regional alliances, particularly its mutual defence treaty with the Philippines, which was ratified in 2014 and broader strategic interests in the Asia-Pacific would ultimately bring it into the conflict. As a result, it is past time to begin taking the cyber threat in the South China Sea seriously. The Philippines, Vietnam, and other targeted countries should devote greater resources to developing more advanced cyber defence infrastructures to protect military systems and other critical networks. This should include adequate funding for national Computer Emergency Response Teams (CERTs) and establishing organisations inside the armed forces to centralise the leadership of cyberspace operations comparable to the United States Cyber Command (Fauzi, 2019).

On a regional level, ASEAN must revive dormant efforts to build a more resilient cybersecurity system to offset the Chinese cyber threat to its members. The organisation should take significant steps to establish a permanent coordinating and information-sharing system, either under the auspices of the ASEAN secretariat or as a stand-alone ASEAN-CERT under the auspices of the Asia-Pacific CERT. While the ASEAN Defense Ministers' Meeting does not currently handle cybersecurity as a separate issue, it would be an ideal venue for better coordinating regional military activities. Furthermore, the ASEAN Regional Forum (ARF), where the Chinese participate, would be appropriate for developing regional codes of conduct and confidence-building measures for cyberspace, increasing transparency and complementing ASEAN-only efforts. ARF should build a communication network that can be triggered during cyber crises, similar to its efforts to improve maritime security. The United States should prioritise enhancing the cyber security capabilities of its regional allies and partners, echoing the sentiment expressed in the recently released U.S. Department of Defense Asia-Pacific Maritime Security Strategy, “both to respond to threats within their territories as well as to provide [security] more broadly across the region" (Diplomat, 2015). This can be accomplished by providing resources, technologies, and training and through collaborative cyber incident response exercises or information-sharing programmes. Increasing the region's cyber defences before the next major crisis provides a realistic paradigm for regional cooperation to progressively make Southeast Asian forces more capable, credible, and autonomous in the cyber world (Gonzales, 2014). It will allow countries to take the lead in securing their territories and networks while gradually relegating the United States to the sidelines.

DISCUSSION

Spratly Islands in Security Threats

The Spratly Islands dispute can be looked at from a variety of angles. In terms of national security, these islands are essential due to their location in the South China Sea, where many merchant ships pass through to deliver goods, people, and energy products to Asian-Pacific countries. By controlling these islands, the country in question would be able to ensure the safe passage of their goods. Regarding energy security, the Spratly Islands are viewed as irreplaceable to nations in the locale because of the expected wellsprings of petroleum gas and oil found under the islands’ seabed. Whichever country wins the dispute would have

the right to explore and develop these resources for domestic consumption. Thus, it would help diversify a country's energy portfolio while making it less vulnerable to foreign oil and gas markets. At this time, however, the amount of recoverable oil and gas that these islands contain has not been fully proven.

Regarding national pride, these islands are significant to countries currently claiming all or part of the islands (Vietnam, China, Taiwan, the Philippines, Malaysia, and Brunei) due to the historical claim these countries have over the territory. These countries have a long seafaring history; however, it has been challenging to say which country first inhabited or used the islands. Altered global power relations further highlight the Spratly Islands dispute. During a speech to the ASEAN Regional Forum in July 2010, U.S. Secretary of State Hillary Clinton stated that the United States has a "national interest" in the region. While the U.S. has no claim in the conflict, the rise of China's economic and military power has jeopardised its influence in the region. China may still not have the same global military reach as the U.S., but the U.S. will no longer have unrivalled dominance in Asia. The United States worries about sustaining global order as the world's leading power. Thus, its interests are not limited to conflict resolution; it is also concerned with maintaining the region's power balance. "The job of global peacekeeping," Womack writes, "is more one of peacekeeping than peacemaking." 100 Finally, the United States' large trade and debt link with China leads the former to deal with the latter warily, despite strong alliances with ASEAN countries, unless it wants to face domestic economic ramifications.

Sea Lanes Security

Sea lane security, at its current time, is famously difficult to define due to the legal, geopolitical, and diplomatic connotations of the term. In the U.N. Convention on the Law of the Sea, all ships are given the right to conduct the innocent passage (unarmed, no unloading of goods or people, and others) of their ships on all territorial sea beds (Part II, Section 3, Subsection A, Articles 17-19). This means that ships can get within 12 nautical miles of a country's coast if they are not a threat to that country's national security. However, tankers or ships carrying hazardous material may be directed to use specialised sea lanes to pass through a country's territorial waters (Part II, Section 3, Subsection A, Articles 22-23).

On the other hand, the laws regarding the passage through straits are more complicated, as they require determining whether the straits from an island are connected to a state's mainland (Mortensgaard, 2015). If they are not connected, ships have a right of transit passage. However, if the straits are connected to a state, other transit passages will be recommended for the security of the state in question (Part III, Section 2, Articles 38-39). The principles of innocent passage in the previous paragraph also apply to the passage of ships through straits. Sea lanes, on this occasion, are the streets of transportation for ships on the ocean and seas. The guidelines above apply to clear cases in which these transportation streets may be impeded or diverted by what they are shipping and what the entry of boats means for a state's public safety. Subsequently, the United Nations Convention on the Law of the Seas offers the country with the islands or regional seabeds unbelievable control. In contrast, countries that rely upon these ocean paths to convey unfamiliar merchandise have a limited impact.

Implication for The Spratly Islands Dispute

For these reasons, the country claiming territorial ownership over the Spratly Islands also gains control of most of the South China Sea (Chang, 1991). This is because their territorial seabeds would extend not from their mainland coastline but from the islands' coastline. For instance, in the map below, China's claim over the islands would make their sea territory extend all the way south to Vietnam, the Philippines, Brunei, Malaysia, and Indonesia (orange line segment), making the "Hypothetical Exclusive Economic Zone (EEZ) limit from coastal states" part of China's territorial waters (Loja,2016). This would not only make it tremendously challenging for Southeast Asians to protest against Chinese naval operations in the future but would also limit their economic activities (fishing, oil and gas exploration and production, shipping) in the "EEZ."

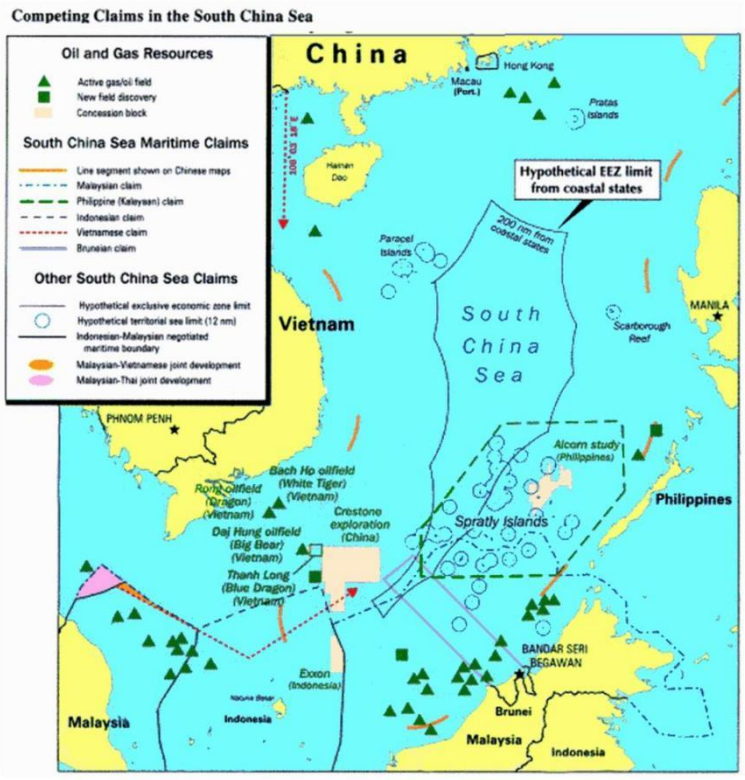

Fig. 1: Exclusive Economic Zone

The territorial claims of the Philippines, Vietnam, Malaysia, Brunei, and Taiwan in the South China Sea are highly contested. China claims nearly the entire territory, including numerous islands and reefs that are technically part of other countries. The precise boundaries of the Chinese claims are uncertain and are commonly known as the "nine-dash line". Nevertheless, the essence of their claim is clear: the SCS belongs to China, according to Beijing.

China Use Cyber to Monitoring Spratly Island

China is bolstering its lead in resource exploration and any conflicts in the South China Sea, a sea disputed by five other governments, by deploying expendable, cost-effective drones. The People's Liberation Army exhibited an "electronic-warfare variant" of drones that had done just reconnaissance missions before, part of an effort to control information during any military movement (Joanna, 2020). Experts say that drones can easily spy because, if caught, operators can claim they are being used for resource exploration. They add that they are cheaper than radars and other intelligence-gathering tools, causing little loss if seized. "The drone is, of course, an ideal sort of spy," said Alan Chong, an associate professor at the S. Rajaratnam School of International Studies in Singapore. "Drones are, in a sense, more expendable than aircraft. If they are shot down, China will raise a protest, but that is it," he added. China, hemmed in by other claimant states and monitored by Western powers, is not expected to occupy more features in the 3.5 million square kilometre sea prized for fisheries and energy reserves (Joanna, 2020). However, drones and other quasi-military technology will help it find undersea fossil fuels and know quickly if another country is expanding, especially near China's existing maritime assets.

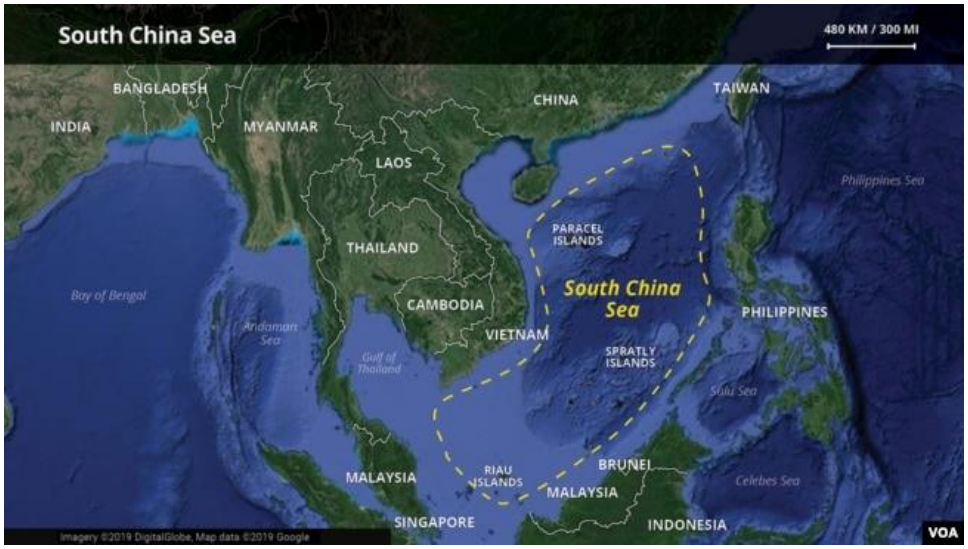

Fig. 2: South China Sea area

Cyber Drones Technology in China

In terms of operation in the South China Sea, "The South China Sea itself is a huge area, so if they want to have a kind of medium-range reconnaissance, I think drones are less expensive and more efficient," said Alexander Huang, a strategic studies professor at Tamkang University in Taiwan. "In a non-hostile situation, I would say for day-to-day operations, it is more cost-effective," he said. Brunei, Malaysia, the Philippines, Taiwan, and Vietnam dispute all or part of China's claims to the sea that stretches from Hong Kong south to Borneo. The United States government, sometimes backed by Japan and Australia, periodically passes naval ships into the sea to check on China's activities, to Beijing's chagrin. China cites historical records to back up its claims to about 90% of the sea (Joanna, 2020).

Drones are traditionally used at sea to check water depths from above the surface, take temperature readings, and even see how much plankton is in the water. Those data help understand marine life and prospects for finding oil or gas. If China is using drones, maybe they want to get ahead by knowing what the potential of these areas is. The area is, of course, affluent in energy resources and other possible economic resources. Images captured by drones can be sent instantly to a base station on a tiny sea islet, minimising the loss of information in case they are captured (Joanna, 2020). China also uses drones to ensure the South China Sea is always its focus. China has developed a fleet of tiny drone ships capable of engaging "shark swarm" foes in sea warfare. It has a fleet of 56 crewless ships on exercises in the South China Sea off the Wanshan Archipelago. Oceanalpha, a Chinese business, confirmed the drones were designed to overwhelm foes in maritime engagements. A mothership commands the armed swarm. Oceanalpha revealed that the Wanshan Marine Test Field was built solely for drone craft training (Barnes, 2018).

Drones are also used tactically in the South China Sea. HiSIBI, a Chinese nautical corporation, announced in December 2017 the construction of the world's fastest drone ship, capable of travelling at 50 knots (58 mph). The new high-speed drone is being tested at the Wanshan Marine Test Field. The test field, still under construction, is expected to be the world's largest, covering around 297.9 square miles. According to military analysts, the unmanned vessel test facility was part of China's broader aspirations to develop autonomous systems for civilian and military applications. The new test site coincides with China's desire to employ technology to protect its maritime interests (Staff, 2018). Researchers at Tianjin University successfully tested the Haiyan autonomous Unmanned Underwater Vehicle at sea (UUV). It has a range of 621.37 miles and can last for 30 days (Lin & Singer, 2014). At the same time that the U.S. Navy is pursuing UUV research to counter China's burgeoning Anti-Access Area Denial capabilities, the Chinese are also developing these capabilities. UUVs can monitor water temperature, conductivity, optical backscatter, and acoustics while covering a larger area and operating more efficiently. Using numerous sensor types in battle mode to detect a stealthy submarine increases the likelihood of discovering the prey (Lin & Singer, 2014). UUVs, as opposed to stationary underwater sonar stations, can be rapidly deployed by ships.

The Haiyan UUV is one of the assets deployed for an Underwater Great Wall, which would be a network of sensors on the seafloor combined with long-endurance UUVs to detect and destroy enemy submarines and mines. The fact that the fish-like Qianlong autonomous underwater vehicle (AUV) can dive to 14,800 feet demonstrates China's interest in deep-sea robotic ships (Katoch, 2018). These UUVs may also strike targets anywhere in the Indian Ocean and collect enemy submarine acoustics and oceanographic conditions to improve stealth and anti-stealth measures. China has created and deployed high-tech drones for population surveillance. These espionage planes, code-named Dove, have flown over 2,000 test flights before being deployed in real-world scenarios. The first bird robots had fixed wings and rotor blades. The Dove drones mimic birds' flapping activity, duplicating around 90% of genuine doves' movements while producing a minimal noise signature. Doves have a wing span of 19.685 inches and weigh only 0.441 pounds. They can fly at speeds of up to 24.855 mph for 30 minutes. China is putting the Doves through facial recognition tests, software stabilisation, explosives arming, and endurance training for targeted assassinations. Swarm formations of drones are being tested (Katoch, 2018). Because of China's aggression and its policy of ambiguity and deceit, the danger is clear and present.

One of the most comprehensive assessments on how the Chinese military uses unmanned drones for force projection and surveillance in the contested South and East China Seas was authored by (McCaslin,2017). China is undergoing a "drone" revolution fueled by massive investment in the Chinese drone sector and unlawful acquisition of foreign drone technology (Katoch, 2018). China places a high strategic value on the South China Sea for cyber network reasons. China has taken an aggressive stance, articulating its sovereignty based on historical claims and developing military and economic facilities on these disputed or reclaimed territories. According to the U.S. Department of Defense, China will create thousands of drones by 2023 (DoD Report, 2015). Drone sightings and accurate identification are critical due to the lack of international norms governing drone treatment, notably in places where sovereignty is contested (Lehman, 2017). The study details four known PLAN drones: the S-100, ASN-209, BZK-005, and GJ-1. Except for the S-100, all are made in China. Scheibel manufactures the S-100 in Austria. The drones under discussion serve a variety of functions, ranging from surveillance (S-100) to military or armed (GJ-1, nicknamed Wing Loong I model) (Lehman,2017).

One constraint on Chinese power projection is their current inventory's inability to launch from the Chinese Navy's lone aircraft carrier. This restricts the ability of the BZK-005 (primary mission surveillance) to be launched from land (McCaslin, 2017). This issue does not affect the S-100, which uses vertical take-off and landing (VTOL) technology. Drones can also be launched from Chinese-controlled artificial islands in contentious areas [such as the Spratly Group] (Lehman, 2017). According to the author, the BZK-005 is suspected of being outfitted with cyber weapons to harass US Naval forces in the Spratly A.O., causing havoc with commercial and maybe U.S. Navy GPS systems. The BZK-005 is a MAME drone that performs specialised surveillance duties. It has an operational ceiling of 26,247 feet, a maximum range of 1491 miles, and a 40-hour endurance. Ground-based runways, such as those in the Spratly Islands group, limit the range. It has electro-optical, infrared, SAR, SIGINT, and satellite communications capabilities, allowing for real-time data transmission. If launched from Chinese-controlled islands (artificial and natural), the BZK-005 range allows surveillance over the whole South China Sea: Woody Island, Subi Reef, Mischief Reef, and Fiery Cross Reef (McCaslin, 2017). The S-100 has a ceiling of 18,000 feet, weighs 75 pounds, is armed with Thales Lightweight Multi-Role Missiles (LMM), has a range of 60 to 125 miles, and can operate for 10 hours. They are typically launched from a frigate of the PLAN Type 054/054A class (McCaslin, 2017). China uses the S-100 for espionage, surveillance, and reconnaissance (ISR). They are outfitted with payloads such as Synthetic Aperture Radar (SAR), Maritime Radar, Signal Intelligence (SIGINT), and Communications Intelligence (COMINT).

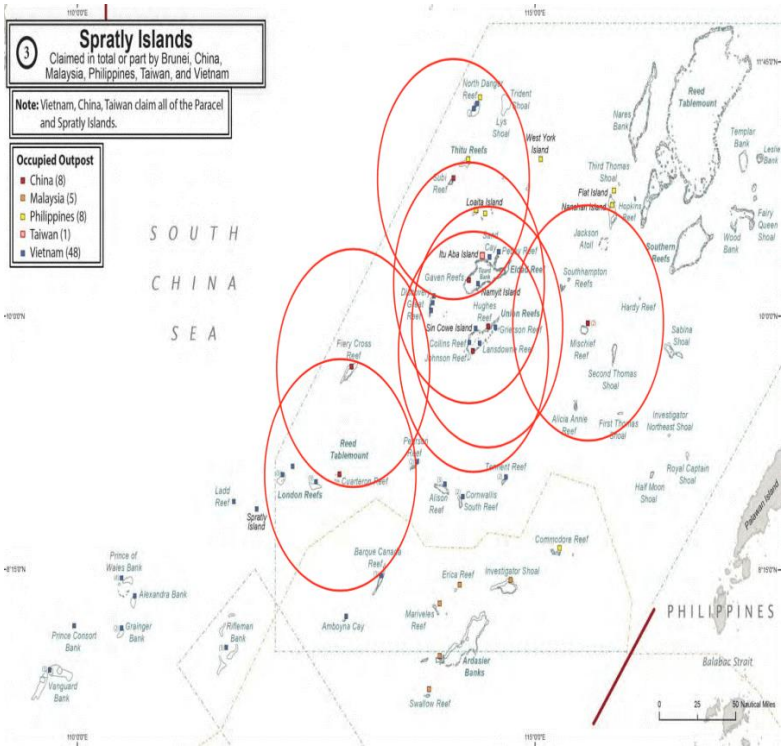

Fig. 3 S-100 Drone Trajectories in the Spratly Islands

The other claimant states, all militarily weaker than China, fret when China improves its maritime technology. Vietnam and China got into a standoff earlier this year over energy exploration tracts off the Vietnamese coast, and Filipinos are growing edgier about China's pressure on their maritime holdings despite friendliness at the state-to-state level. People are concerned that China is using technology in the South China Sea and spying on the Philippine population in general (Loja, 2016). China does not disclose details about its drone deployments, but it has indicated that it sees drones as necessary hardware in the maritime dispute.

These drones are connected to many ground controllers and satellite communications links to remotely pilot and control them. These networks are connected via cyber technology. The remote control system, communications, sensors, and mechanical aspects are controlled by computers and, in some instances, by artificial intelligence (A.I.). These pose vulnerabilities for the drones to be manipulated by hacked systems or brought down by sabotage. In other words, China's drones can be remotely controlled or monitored using cyber means. Cyber malware and Trojan horses can covertly infiltrate the drone network and systems through internet or intranet connection nodes or human interfaces. Once infiltrated, the drones' feed can be monitored and even manipulated. Nonetheless, China also has formidable cyber security technologies, and its drones and cyber network are expected to be well protected. Therefore, future research on China's cyber defence will need to be conducted to learn lessons on how to protect a drone network of systems and how to exploit its potential vulnerabilities.

CONCLUSION

Thus far, bilateral agreements have been the only approach to pacify this conflict. However, this approach breeds distrust as countries immediately place their national sovereignty first by creating overlapping yet contradictory agreements. For example, this can most recently be illustrated by the agreement signed by Vietnam and China (October 11, 2011) to hold biannual talks on border disputes and establish an emergency hotline for the South China Sea. Nevertheless, simultaneously, Vietnam aligned itself with India on October 13, 2011, to explore the South China Sea for oil and natural gas.

What is needed to resolve this dispute is multilateral talks by all the parties involved in the conflict. This would establish a mutual foundation of understanding and send a message to the countries involved that there is a willingness to compromise and work together. In terms of operation, drones are less costly

and more efficient. Day-to-day operations costs are higher and irrelevant for such operations. Drones offer a cost-effective monitoring solution and can also analyse the data they capture, simplifying their application. The systems were developed for civilian and military applications as part of tactical. Also, networks of sensors on the seafloor were combined to detect and destroy enemy submarines and mines. The strategic advantages that are very clear in the South China Sea for China are part of the border that belongs to China itself. That is an advantage for China in many aspects.

Drones are a tool that helps facilitate business and get information. Controlling Chinese drones over the South China Sea, for example, can assist China in learning more about the activities in each territorial water. China's drones depend on cyber technology for control, communications, and operations. Hence, China's use of drones to monitor the South China Sea has given it an operational, tactical, and strategic advantage, but at the same time, it has created potential weaknesses and vulnerabilities for sabotage. Further in-depth research by the authors will be required in this critical area, drones with cyber.

Acknowledgements

The author expresses his gratitude to the Malaysian Ministry of Higher Education for a generous Fundamental Research Grant Scheme (FRGS/1/2020/SS0/UPNM/02/1), which enabled the authors to conduct their research for this article.

REFERENCES

Barnes, T (2018) China Tests Army of tiny drone ships that can 'shark swarm' enemies during sea battles. Independent. Retrieved September 12, 2022, from https://www.independent.co.uk/news/world/asia/china-drone-ships-unmanned-test-video-military-south-sea-shark-swarm-a8387626.html

Chang, T. K. (1991). China's Claim of Sovereignty over Spratly and Paracel Islands: A Historical and Legal Perspective. Retrieved April 19, 2022, from https://core.ac.uk/download/pdf/214079615.pdf

Diplomat, A. P. (2015). The Chinese cyber threat in the South China Sea. – The Diplomat. Retrieved September 14, 2022, from https://thediplomat.com/2015/09/the-chinese-cyber-threat-in-the-south-china-sea/

DoDReport https://www.defense.gov/portals/1/documents/pubs/2015_china_militaryPower_report.pdf

Fauzi, N. (2019, April 19). *Cyber threat: Are we ready?* ISIS. Retrieved April 20, 2022, from https://www.isis.org.my/2017/09/14/cyber-threat-are-we-ready/

Gonzales, R. (2014). The Spratly Islands Dispute: International Law, conflicting claims, and Retrieved September 14, 2022, from https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1094&context=award

Hayton, B. (2014). The South China Sea: The Struggle for Power in Asia. Retrieved April 17, 2022, from https://www.researchgate.net/publication/272367596

Joanna, F. (2020). *The use of drones over the South & East China Seas*. droneswar.net. Retrieved April 25, 2022, from https://dronewars.net/wp-content/uploads/2020/10/DW-CrowdedSky-WEB-1.pdf

Katoch, P.C, Gen (2018) New Chinese Drones – formidable challenge. SPSMAI.Retrieved September 12, 2022,fromhttps://spsmai.com/experts-speak/?id=556&q=new-chinese-drones-formidablechallenge

Lehman, C.F. (2017) Report: China Increasing Drone Operations in Disputed Seas, Freebeacon. Retrieved September 12, 2022, from http://freebeacon.com/author/charles-lehman

Lin, J & Singer, P.W. (2014) Not a Shark, But a Robot: Chinese University Tests Long-Range Unmanned Sub. Popular Science. Retrieved September 12, 2022, from https://www.popsci.com/blog network/easter-arsenal/not-shark-robot-chinese-university-tests-long-range-unmanned-mini-sub#page-3

Loja, M. H. (2016). The Spratly Islands as a single unit under international Law: A commentary on the final Award in Philippines/China Arbitration. Retrieved April 19, 2022, from https://www.tandfonline.com/doi/abs/10.1080/00908320.2016.1229936?jjournalsode=uodl20

McCaslin, I.B. (2017) Red Drones over Disputed Seas: A Field Guide to Chinese UAVs/UCAVs Operating in the Disputed East and South China Seas. Released by Project 2049 Institute at http://project2049.net/documents/Red%20Drones%20over%20disputed%20seas_PLA_project2049.pdf

Mortensgaard, L. A. (2015). The Spratly Islands Dispute – A Discourse Analysis. Retrieved April 15, 2022, from https://www.e-ir.info/2015/07/19/the-spratly-islands-dispute-a-discourse-analysis

Staff writer. (2018), China starts work on world's biggest test site for drone ships near the South China Sea. Today. Retrieved April 20, 2022, from https://www.todayonline.com/world/china-starts-work-worlds-biggest-test-site-drone-ships-gateway-south-china-sea

United Nations Convention on the Law of the sea. (2019). Retrieved April 20, 2022, from https://www.imo.org/en/OurWork/Legal/Pages/UnitedNationsConventionOnTheLawOfTheSea.aspx

United Nations Convention on the Law of the Sea. (n.d.). Retrieved April 20, 2022, from https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf