RESEARCH ANALYSIS
JANUARY 2018

CYBER-ATTACKS AND HYBRID CHALLENGES IN THE SOUTH CHINA SEA

MARCO MALDERA

UNIVERSITÀ DEGLI STUDI FIRENZE

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

CYBER-ATTACKS AND HYBRID CHALLENGES IN THE SOUTH CHINA SEA

Marco Maldera

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

January 2018

ABOUT THE AUTHOR

He holds a bachelor's degree in International Studies from the "Cesare Alfieri" Political Sciences School in Florence, where he graduated with a thesis on China-Ethiopia relations. From the same university, he holds a master's degree in International Relations and European Studies. His thesis focused on economic intelligence in Italy, ten years after the intelligence services reform. He is now attending a second-level master's degree in Foreign Trade and Internationalisation of Businesses at the "Tor Vergata" University of Rome. He is particularly interested in China, intelligence and securitising thematics.

CYBER ATTACKS AND HYBRID CHALLENGES IN THE SOUTH CHINA SEA

Introduction

In a world in constant and ever faster transformation, the man-made cyber domain has already affirmed as one of the main actors of the third millennium. Information, communications and technology will be more and more closely linked to the internet and to the cyber domain. Modern computers can elaborate and transmit huge amounts of data and information in real time, making communications extremely fast.

ICT itself has no universally accepted definition because concepts, methods and applications involved see a constant evolution taking place on an almost daily basis. The number of people using computing tools has grown bigger and bigger, while technology has seen a shift: in the past military technologies have affected the civil behavior, while today there is no clear division between the military and the civil level, as cyber involves every part of our daily life. But do we actually realize what kind of impact does the cyber domain have on our lives? Are there any concrete examples concerning this topic or is it all just theory, with practice that still has to be seen? Do States use this new tool, and how does it work compared to the traditional ones? What is their role and how well do they perform?

In this brief analysis we will try to understand in which way States are involved in the cyber domain, and how this is relevant for the daily life both of common citizens and for the State itself, if it be can considered an issue involving its own national security. In particular, the case analyzed will be the one of the South China Sea, in which many countries of the region have disputes over portions of this area, where China is building some artificial islands and is conducting cyber operations, emerging as primary actor.

As challenges are more and more complex, another issue which adds to cyber operations is the one carried out by the so called '*maritime militia*',

a civilian fishing fleet with strong ties with the People's Liberation Army playing an active role in the South China Sea.

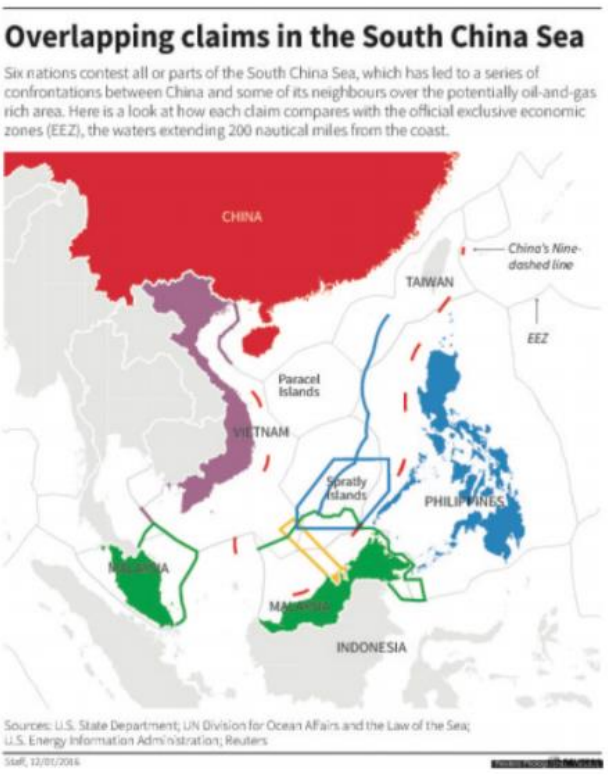
The evolution of war: the cyber domain

Until few decades ago the most common type of war fought among States was the traditional one, involving its military and, in some cases also it's civil society. Even though most developed countries carry out conflicts also in other ways, it is necessary to realize that the nature of war has never stopped changing: Carl von Clausewitz, considered one of the fathers of strategic studies, said that war is like a chameleon, meaning that its nature changes all the time and every conflict is unique. Even though the European continent is living in the longest period of peace since World War II, today there are many conflicts going on at global level. Many States still use traditional weapons, such as tanks and airplanes, but the hard-military ones are not the only tools to fight a conflict.

Recently another weapon has emerged as extremely efficient: the computer. This has proved itself to be so efficient that the NATO summit held in Warsaw in July 2016 recognized cyber as the fifth domain of confrontation, joining the traditional ones, namely land, sea, air and space. Despite the importance of such fact, it must be noted that at international level there is no clear definition of concepts such as the ones of '*ICT*' and '*cyber*'. Chinese for example, do not talk about *cyber* as the West does, but talk about *informatisation*, and also for this reason, Beijing's approach to *information security* is so restrictive and control-seeking (Warsaw summit communiqué 2016). The fact that the result of the NATO summit is an important statement such as the one of the fifth domain implies that such tool has already seen its first use. In fact, many countries around the world have already faced an attack by this cyber weapon: in Europe there is the case of Estonia, in 2007 (Nbc News 2009), while the United States has probably been attacked during the 2016 presidential elections that brought Donald Trump as the 45th U.S. President at the White House (ABC News 2016). However, the first use ever of the digital weapon can be dated back to 2010, concerning the Stuxnet virus, which targeted auranium enrichment plant in Iran. The importance of such attack is that it escaped the digital realm to wreak physical destruction on equipment and the computers controlled. This means that the cyber tool produces effects also in the 'real' world and

not just in cyber space (Zetter 2014). The Asia-Pacific has been involved too, as there has been the case of cyber-attacks against many coastal countries in the South China Sea (Gertz 2015).

An essential element that marks the difference between the cyber weapons and the traditional ones is the reason for which such tool is so efficient: one of the most important features of the cyber domain is anonymity, as it is extremely difficult to provide evidence on who was using the gun that "opened fire". Anyhow in the case concerning the South China Sea, the digital conflict still going on assumingly carries the sign of the alleged author of the attacks as such moves can be tracked to geopolitical reasons. A very active actor in such portion of the sea is China which, like other coastal countries of the area, has claims on these waters and on the ones of the East China Sea.



Claims on the South China Sea

Anyway, it is the South China Sea which represents the core of Beijing's claims that is fiercely competing with its regional rivals, namely Brunei, Malaysia, the Philippines, Taiwan and Vietnam, over vast swaths of the waters rich in oil, natural gas, and fisheries. The roots of the disputes are based on what China calls the 'Nine-Dash Line', concerning about 90% of these waters (Goel 2016), affirming its historical rights on them.

The concept of the 'Nine-Dash Line' has its origins in 1947, when the Chinese Nationalist Government had drawn an eleven-dotted line. This was based on China's maximum period of maritime influence, which ended with the arrival of the Portuguese in the 15th Century (Cordesman & Kendall 2016, p. 583).

Beijing is convinced about its property on such a huge amount of water, reason for which it has started building artificial islands in the area. These can be used both for civil and military purposes, which is another cause of tension. Given the difficulties in distinguishing between the two spheres, Beijing believes that this makes it easier to legitimize its control over the area without using hard power, as it says that the military infrastructures are necessary to provide security for the civil ones (Miracola 2017).

To this, it must be added the fact that about US$3.4 trillion dollars of goods flow through the disputed region annually, making the sea a major strategic target for China to control. These factors bring to an increase of the countries involved in the area, such as the United States promoting freedom of navigation and Japan, for obvious security concerns.

For these reasons, the South China Sea today constitutes the primary global hotspot where major and regional power's vital interests and alliances commitments directly clash (Center for Strategic and International Studies 2017).

The two images show the infrastructures built on one of the Chinese man-made islands and how its airstrip and aircraft capabilities compare to the ones of other countries.

All these facts explain Beijing's claims on the South China Sea, but how are these linked to the cyber domain? How are cyber tools used? When was the first attack carried out?

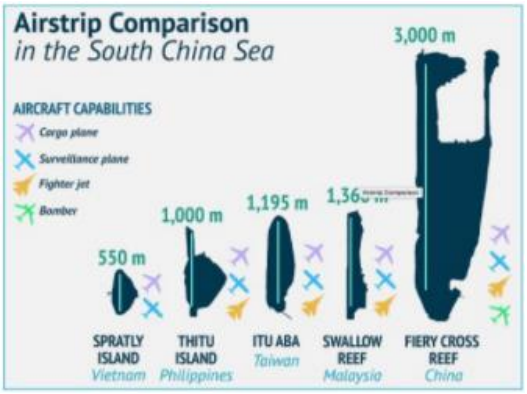
Beijing has announced that any attempt to counter its claims represent a threat to its core national interests: for this reason, it has carried out cyber-attacks on regional states along with political influence operations designed to falsely convince the international community that such waters are and have been China's sovereign maritime territory (Gertz 2017).

Regional tensions and some of the most important cyber attacks

Beijing's first White Paper on Military Strategy published on May 26, 2015, states that China seeks '*peaceful development, [...] oppose*

hegemonism and power politics in all forms, and will never seek hegemony or expansion'. Anyhow, in the same document it is possible to read that China is '*building itself into a maritime power. [...] The traditional mentality that land outweighs sea must be abandoned, and great importance has to be attached to managing the seas and oceans and protecting maritime rights and interests*'. The document states that China is looking for a '*combination of "offshore waters defense" with "open seas protection"*', as the former is not sufficient any longer: it is the '*going blue*' strategy, which has the aim to extend naval operations from nearby waters to the open oceans.

Beijing is flexing its muscles in the world's seas as it has started establishing foreign naval bases (India Times 2018), but it also wants to become a global power and its efforts begins from imposing regional hegemony and changing Asia's strategic balance (Gertz 2017).



No country was spared, as the targets have included government entities in Cambodia, Indonesia, Laos, Malaysia, Myanmar, Nepal, the Philippines, Singapore, Thailand, and Vietnam as well as international bodies such as the United Nations Development Program (UNDP) and the Association of Southeast Asian Nations (ASEAN) (Gertz 2015). The Permanent Court in The Hague has been targeted too, as its website went offline in October 2015, probably due to Chinese hackers that have breached the Court's servers during a hearing on the territorial dispute brought by the Philippines (Goel 2016).

Cyber-attacks characteristically follow the timing of heightened geopolitical tensions (Goel 2016). Erka Koivunen, advisor in the Finnish

cyber-security company F-Secure, talked about Advanced Persistent Threat (APT) and explained: "*Not only are the targeted organizations all related to the case in some way, but its appearance coincides chronologically with the publication of news or events related to the arbitration proceedings*" (Perez 2016): context and timing serve as damning evidence (Piiparinen 2016).

One of the first cyber campaigns occurred in April 2012, following a tense standoff between Chinese and Filipino naval vessels around the Scarborough Shoal. A Chinese cyber unit breached government and military networks, stealing highly sensitive data related to the conflict (Piiparinen 2016). Manila was also the target of one of the most important cyber-attacks: on July 12, 2016, within hours of the Permanent Court of Arbitration's unanimous rejection of China's claims in the South China Sea, at least 68 national and local government websites, among which the Department of Foreign Affairs, the Department of National Defense, the Central Bank, and the Presidential Management Staff, along with a medical center and smaller local government units, were knocked offline in a massive distributed denial of service (DDoS) attack. The Court has rejected all Chinese claims finding that none of Beijing's requests have legal bases: neither the historic rights over the Nine-Dash Line nor the exclusive economic zone ones. Chinese foreign ministry dismissed the Court's award, saying it has no binding force (Piiparinen 2016). It is clear that the region faces a challenge over whether might or right will determine the rules (Cronin 2016, p. 9).

Another target of many cyber-attacks is Vietnam, as together with the Philippines it is the most vocal in criticizing China for its increased assertiveness over the area. Vietnam has been involved because on July 29, 2016, a few days after having moved its rockets to fortify some of the islands in the disputed South China Sea, the flight screens on two of the country's biggest airports displayed messages critical of Hanoi's claims to the contented waters (Goel 2016). According to the cyber security firm FireEye, there are '*cyberspies working for or on behalf of China's government*', as the firm has traced a cyber-attack coming from suspected Chinese cyber-spies: evidences are '*based partly on the fact that a Chinese group it had identified previously had used the same infrastructure before*'. Obviously, Chinese Foreign Ministry representative Hua Chunying said Beijing opposes any accusation from any country without cast-iron proof (First Post 2017). China asks for

evidence well aware that cyberspace's anonymity makes the task extremely difficult.

Tension between China and Vietnam are at its highest in about three years over the disputed South China Sea, as Hanoi suspended oil drilling in offshore waters in July 2017 under Beijing's pressure. China also appeared uneasy at Vietnam's effort to rally Southeast Asian countries over the South China Sea (First Post 2017).

Hacking attacks have been concerning also South Korea's government, military and defense companies because of the country's deployment of a U.S. missile-defense system, the Terminal High-Altitude Area Defense (THAAD), aimed at defending the State from a North Korean missile threat. China opposes THAAD, saying its radar system can reach deep into its own territory and compromise its security (Cheng & Chin 2017).

Anyhow, one of the most important States involved in Chinese claims in the area is Taiwan, used as a testing ground for cyber-attacks that are then directed towards larger countries. Beijing considers the island as a renegade province it must recover, so it is an ideal target for Chinese hackers as it is close to the mainland, mandarin-speaking and boasts advanced internet infrastructure (Gold 2013). The "*China's New Map of Greater China*", released in June 2014, gave Beijing the areas claimed by Vietnam, the Philippines and other countries and included Taiwan as part of China's territory too (Cordesman & Kendall 2016, p. 583); this was followed by the 2015 Military Strategy which stated that '*the Taiwan issue bears on China's reunification and long-term development, and reunification is an inevitable trend in the course of national rejuvenation*' (Ministry of National Defense 2015).

A common pattern in these attacks is that hackers, just like in intelligence operations, went in stealthily to acquire or manipulate information, rather than to cause disruption (Gold 2013).

According to Bryce Boland, FireEye's Asia-Pacific chief technology officer, "*many governments and militaries in Southeast Asia lack cyber security controls that can effectively match these elevated threats*" (Vasagard & Dyer 2016). According to Truong Minh Tuan, Vietnam's minister of information and communications, the government is reviewing Chinese technology and devices after the July cyber-attack, as the country's major telecom operators uses Chinese technology, raising threats of more data breaches (Japan Times 2016). This leads to very

relevant security issues, as Chinese hackers gained strategic access to foreign State's computer networks that could be shut down in case of crisis, or used to spread disinformation internally to confuse and weaken China's enemies. Southeast Asian claimants remain unprepared to counter Chinese hackers with operational cyber capabilities '*that are weak at best and completely non-existent at worst*', reason for which they should begin rapidly investing in more sophisticated cyber capabilities '*through national investments, regional initiatives, and broader international defense cooperation*' (Piiparinen 2017).

But cyber-attacks are not all, as according to the Hong Kong-based South China Morning Post, China has established an underwater surveillance network which will help its navy track target vessels more accurately and give it a cutting edge in the Indian Ocean and the South China Sea. The Post says that '*The project [...] is part of an unprecedented military expansion fuelled by Beijing's desire to challenge the United States in the world's oceans*' (India Times 2018).

Anyhow, it is not just Beijing carrying out cyber-attacks in the South China Sea, as according to Bryce Boland, FireEye chief technology officer for Asia Pacific, hackers linked to Vietnam too are doing the same against Philippine state agencies in order to gather information concerning the disputed waters. Boland said that the hackers, called APT32 "*are aligned to the interests of the Vietnamese government*" (Reuters 2017b).

The power and the prestige of the Communist Party of China (CPC) depends also on its ability of keeping the territorial integrity, point on which Beijing is not willing to make steps back. On August 1st, 2017, during a military parade for the celebrations of the 90th anniversary of the founding of the People's Liberation Army, President Xi, chairman of the Military Commission, stated: "*We do not allow any individual, any organisation, any political party, at any time or by any means, to split any single piece of the Chinese territory [...] No one could expect us to swallow consequences that damage our sovereignty, security and developmental interests*" (Zhen 2017).

Several images were produced for the event, all showing, as part of Chinese territory, also Taiwan and the area claimed in the South China Sea.

Smoking guns and overheating devices: the authors of the cyber attacks

Tracking the exact source of the attacks is a slippery game and it remains unclear to what extent the attacks were directed, encouraged, or merely tolerated by Beijing. Anyhow, one very important hint indicating government's support in such operations are the author's capabilities: unlike common hackers, States dispose of great amounts of capitals, skills and time needed to prepare a successful attack. Moreover, according to a Taiwan expert in cyber espionage, hackers "work very normal hours – on Chinese national holidays, for example, we don't see any hacking activity at all" (Gold 2013). According to the 2016 NATO report, the independent group Red Hacker Alliance could be composed by several hundred thousand members and, given the large quantity of stolen data available, their actions are tolerated and most likely supported by the government (Raud 2016, p. 26). On its side, Beijing reverses the accuses saying it is 'one of the major victims of hacker attacks' itself, reason for which it is working on its cyber capabilities that have the aim to 'maintain national security and social stability' (Ministry of National Defense 2015). For this purpose, China's cyber capabilities keep evolving, but some authors have noted that this is going on in parallel with military modernization: Unit 61398 and Unit 78020 are just two examples of Shanghai-based People's Liberation Army (PLA) hacking groups (Raska 2017). Science of Military Strategy, a book issued by the Academy of Military Sciences, PLA's most important research institution, emphasizes conflict in the network domain. It openly states that China disposes of specialized network warfare units operating within both the military and the civilian spheres, carrying out offensive and defensive cyber operations (Raud 2016, p. 19). The 2015 Military Strategy explicitly stated 'the armed forces will continue to follow the path of civil-military integration (CMI), actively participate in the country's economic and social construction' calling for civil-military partnerships in key sector.

Sun Tzu: old but gold. Ancient advices applied in the cyber domain

Concerning military strategy, the Chinese cannot ignore the *Art of War*, a text written by Sun Tzu 2,500 years ago and valid still today as it emphasizes speed, surprise, asymmetry and economy of force. It is easy to notice how all these characteristics can be found in the cyber domain too (Geers 2011, p. 3). In a chapter, Sun Tzu (2000, p. 16) says:

> *"There are not more than five musical notes, yet the combinations of these five give rise to more melodies than can ever be heard. [...]*
> *In battle, there are not more than two methods of attack—the direct and the indirect; yet these two in combination give rise to an endless series of maneuvers".*

Sun Tzu highlights the importance of combinations, which today can be composed by an astonishing number of factors: not just the direct and indirect attack, but also the fact that today there is no distinction between the civil and the military sphere as cyber strictly links the two; cyber weapons are used with the traditional ones (they do not take their place); the use of asymmetric warfare; the uncertainty that lies behind the authors of the cyber-attacks.

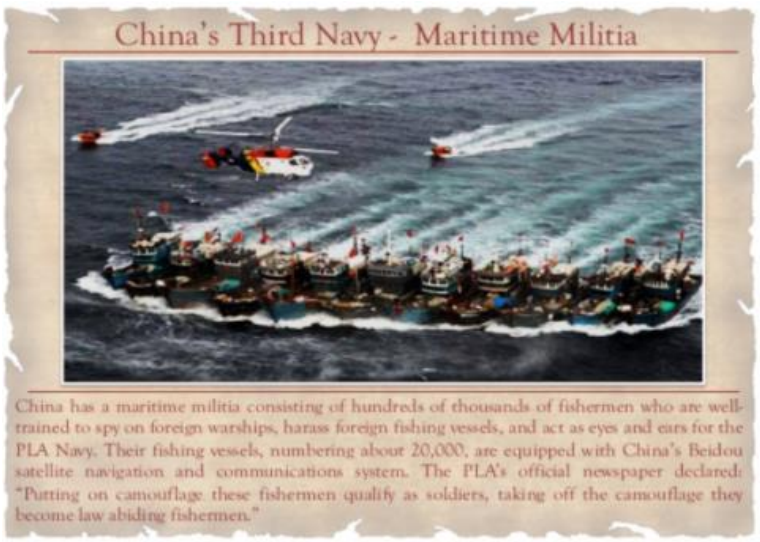
Just like in the cyber domain, the core of the hybrid warfare is given by a great number of different combinations with a huge firepower, many of which can be seen today in the South China Sea.

Anyhow, the foundations of Chinese thinking of asymmetric warfare, including cyber-war, was laid down in a 1999 book, *Unrestricted Warfare*. The two authors, PLA colonels Qiao Liang and Wang Xiangsui provided a strategy of how China as a weaker country could defeat a technologically superior foe outside the scope of using hard military power (Raud 2016, p. 9).

Thanks to cyber weapons, Beijing is winning the war in these disputed waters in the best way possible, as according to Sun Tzu: "*Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting*" (2000). This is just what is happening, as by conducting cyber-attacks along with political influence operations, Beijing is winning without firing a shot.

The maritime militia

In addition to its regular maritime actors, the People's Liberation Army Navy (PLAN) and the Chinese Coast Guard (CCG), Beijing has also a third sea force, the Chinese Maritime Militia (CMM), officially a fishing fleet. Anyhow, according to a Pentagon's report, the maritime militia is engaged in '*low-intensity coercion in maritime disputes*' as China uses it '*to enforce maritime claims and advance its interests in ways that are calculated to fall below the threshold of provoking conflict*' because '*confrontational operations short of war can be an effective means of accomplishing political objectives*'. It represents a paramilitary force masquerading as a civilian fishing fleet and is a weapon for gray zone aggression (Pickrell 2017). By analyzing Chinese-language open sources,



Conor Kennedy and Dr. Andrew S. Erickson have seen that Beijing boasts the world's largest fishing fleet and part of the thousands people working on fishing vessels and in the related industries are registered in the Maritime Militia which have played an active role in numerous sea accidents. This operates both in coordination with and independent of the PLA and, according to Kennedy and Erickson, the group is "*thus a state-organized, -developed, and -controlled force operating under a direct military chain of command to conduct Chinese state-sponsored activities" as they receive "military training directly from uniformed PLAN personnel while wearing their own militia uniforms*" (2017, p. 2-4, 9, 15).

By using civilian craft and personnel, China is avoiding direct military-to-military confrontations and gaining an element of deniability. Some have referred to the maritime militia as the "*little blue men*", lacking a clear identification just like in the case of 2014 Russia's "*little green men*" in Crimea and Ukraine (Tisdall 2016). A 2016 article of China's Militia described one of the militia's requisite characteristics as: '*putting on military uniforms [they] qualify as soldiers, taking off the uniforms they qualify as citizens*'.

Conclusions

One of the issues with cyber security is not whether a system is safe or not, but how protected and vulnerable it is. Another problem we are called to deal with is the anonymity that characterizes cyber domain, as it is not possible to provide absolute evidence on the authors of cyber-attacks.

This is exactly the case of the issue concerning States and international organizations targeted for the disputes related to the South China Sea. Links with the Chinese government have been found, but some hints do not provide a certain evidence. Anyhow, there is no doubt that these cyber-attacks promote political goals favorable to China. If the government itself is not the author of the attacks, it is not clear what its role is and how informed it is on what is going over this issue.

Beijing has many claims in the area, the most important of which is its territorial integrity that includes Taiwan, seen as a renegade province it must recover. China's biggest problem in terms of global and security affairs is not the South China Sea, but the reunification with Taiwan, as on this small island Chinese and US strategic interests collide. If the possibilities of a traditional conflict for this issue are quite remote, the militarization of cyber space is growing at a very fast rate.

Already today, even though it is not that evident, the place where different interests collide is the cyber space, as it gives the possibility to attack without being identified, so the real issue here is the one of cyber security.

States dispose of great amounts of capitals and skills, which makes them the perfect actor capable of manipulating information, both at national level, involving its own citizens, and on the international arena. As dependence on IT and the Internet grows, governments should make proportional investments in network security, incident response, technical training and international collaboration. But a very big issue concerning the cyber domain is that it evolves extremely rapidly, making it almost impossible for international norms and laws to keep up, also because sometimes there is no universally accepted definitions, just like in the case of the terms "cyber" and "ICT", making it very complicated for States to cooperate on these issues that have an enormous impact on the everyday life, both of the single individuals and for the States itself, providing a relevant concern in terms of national security.

Just like cyber actors, another very relevant subject is playing an active role in the South China Sea and by doing so it is contributing to create a higher degree of uncertainty in the area. This is the Chinese Maritime Militia, officially a civilian fishing fleet that has strong links with the People's Liberation Army, as one of its tasks is to support it in defending China from external threats.
As if the cyber security issue were not enough, the maritime militia with its unclear civil-military role, makes this hybrid and unconventional challenge even more uncertain.

References and bibliography

Book: online

Cordesman A. H., Kendall J, (December 2016) *Chinese strategy and Military modernization in 2016. A comparative analysis*, Final review edition December 5, 2016, Center for Strategic and International Studies. Available from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/161208_Chinese_Strategy_Military_Modernization_2016.pdf. [Accessed 7 July 2017].

(2000) *Sun Tzu on the Art of War. The oldest military treatise in the world*, England, Allandale Online Publishing. Available form https://sites.ualberta.ca/~enoch/Readings/The_Art_Of_War.pdf. [Accessed 12 November 2017].

Report

Kennedy C. M. & Erickson A. S., (March 2017) *China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA*, China Maritime Studies Institute Center for Naval Warfare Studies U.S. Naval War College, China Maritime Report No. 1. Available form http://www.andrewerickson.com/wp-content/uploads/2017/03/Naval-War-College_CMSI_China-Maritime-Report_No-1_People%E2%80%99s-Armed-Forces-Maritime-Militia-Tethered-to-the-PLA_Kennedy-Erickson_201703.pdf. [Accessed 9 October 2017].

Journal article: online

Cronin, P. M., (November 2016) Power and Order in the South China Sea, A Strategic Framework for U.S. Policy, *Center for a New American Security*. Available from https://www.cnas.org/publications/reports/power-and-order-in-the-south-china-sea. [Accessed 31 January 2018].

Raud M., (2016) *China and Cyber: attitudes, strategies, organization*, NATO Cooperative Cyber Defence Centre of Excellence. Available from https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf. [Accessed 31 January 2018].

Web page

ABC News (10 December 2016) *CIA finds Russia interfered to help Donald Trump win US election: reports*.
Available form http://www.abc.net.au/news/2016-12-10/russia-interfered-in-us-elections-to-get-trump-elected-report/8109106.
[Accessed 27 August 2017].

Center for Strategic and International Studies (2 August 2017) *How much trade transits the South China Sea?*.
Available from http://chinapower.csis.org/much-trade-transits-south-china-sea/. [Accessed 9 December 2017].

Cheng J. and Chin J., (21 April 2017) *China's Secret Weapon in South Korea Missile Fight: Hackers*.
Available from https://www.wsj.com/articles/chinas-secret-weapon-in-south-korea-missile-fight-hackers-1492766403. [Accessed 21 December 2017].

Gertz B., (27 September 2015) *Unit 78020: New PLA cyber attack unit linked to Beijing's South China Sea takeover campaign*. Available from http://flashcritic.com/unit-78020-new-pla-cyber-attack-unit-linked-to-south-china-sea-takeover-campaign/. [Accessed 8 August 2017].

Gertz B., (10 January 2017) *How China Wins the South China Sea War (Without Firing a Shot).* Available from http://www.atimes.com/china-wins-south-china-sea-war-without-firing-shot/. [Accessed 29 October 2017].

Goel A., (12 August 2016) *The Great Cyber Game in South China Sea.* Available from https://cyware.com/news/the-great-cyber-game-in-south-china-sea-883f7f39. [Accessed 16 November 2017].

Gold M., (18 July 2013) *Taiwan a 'testing ground' for Chinese cyber army*. Available from http://www.reuters.com/article/net-us-taiwan-cyber-idUSBRE96H1C120130719. [Accessed 30 July 2017].

India Times (1 January 2018) *China's surveillance network can easily locate targets in Indian Ocean*. Available from https://economictimes.indiatimes.com/news/defence/chinas-surveillance-network-can-easily-locate-targets-in-indian-ocean/articleshow/62325858.cms. [Accessed 2 February 2018].

Japan Times (10 August 2016) *Spyware attacks Vietnamese government sites amid South China Sea dispute*. Available from http://www.japantimes.co.jp/news/2016/08/10/asia-pacific/spyware-attacks-vietnamese-government-sites-amid-south-china-sea-dispute/#.WRAxk2nyiih. [Accessed 8 July 2017].

Kenneth G., *Sun Tzu and Cyber War*, (9 February 2011) Naval Criminal Investigative Service (NCIS), Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn, Estonia, p. 3. Available from https://ccdcoe.org/sites/default/files/multimedia/pdf/Geers2011_SunTzuandCyberWar.pdf. [Accessed 26 November 2017].

Ministry of National Defense (26 May 2015) *Full Text: China's Military Strategy*. Available from http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm. [Accessed 7 February 2017].

Miracola S., (5 aprile 2017) *All'ombra del vertice il confronto strategico tra Cina e Stati Uniti*. Available from http://www.cinaforum.net/mar-cinese-meridionale-thaad-trump-xi/. [Accessed 8 August 2017]

NATO (9 July 2016) *Warsaw summit communiqué*, last updated 29 March 2017. Available from https://www.nato.int/cps/en/natohq/official_texts_133169.htm. [Accessed 16 December 2017].

NBC News (8 July 2009) *A look at Estonia's cyber attack in 2007*. Available form: http://www.nbcnews.com/id/31801246/ns/tecnology_and_science-security/t/look-estonias-cyber-attack/. [Accessed 29 October 2017].

Perez R., (4 August 2016) *Advanced malware linked to South China Sea cyber-attacks.* Available from https://www.scmagazineuk.com/advanced-malware-

linked-to-south-china-sea-cyber-attacks/article/530587/. [Accessed 8 August 2017].

Pickrell R., (8 June 2017) *China has a covert naval fleet disguised as fishing boats*. Available from http://www.businessinsider.com/china-has-covert-naval-fleet-disguised-fishing-boats-2017-6?IR=T. [Accessed 29 October 2017].

Piiparinen A., (22 July 2016) *China's Secret Weapon in the South China Sea: Cyber Attacks*. Available from http://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/. [Accessed 29 November 2017].

Piiparinen A., (12 July 2017) *Phishing in the South China Sea: Cyber Operations and Hybrid Warfare in the Troubled Waters*. Available from https://www.chinausfocus.com/peace-security/phishing-in-the-south-china-sea-cyber-operations-and-hybrid-warfare-in-the-troubled-waters. [Accessed 2 February 2018].

Raska M., (8 March 2017) *China's evolving cyber warfare strategies*. Available from http://www.atimes.com/article/chinas-evolving-cyber-warfare-strategies/. [Accessed 8 August 2017].

Reuters (25 May 2017b) *Vietnam-linked hackers likely targeting Philippines over South China Sea dispute: FireEye*.
Available from https://www.reuters.com/article/us-cyber-philippines-southchinasea/vietnam-linked-hackers-likely-targeting-philippines-over-south-china-sea-dispute-fireeye-idUSKBN18L1MR.
[Accessed February 1, 2018].

Reuters, (31 August 2017a) *Amidst heightened tensions in South China Sea, China broadens cyber attacks on Vietnam: FireEye*. Available from http://www.firstpost.com/tech/news-analysis/as-tension-over-south-china-sea-strengthens-state-sponsored-chinese-cyberattacks-on-vietnam-increase-fireeye-3992689.html. [Accessed 31 August 2017].

Tisdall S., (16 May 2016) *Little blue men: the maritime militias pushing China's claims*. Available from
https://www.theguardian.com/world/2016/may/16/little-blue-men-the-maritime-militias-pushing-chinas-claims-in-south-china-sea [Accessed 29 October 2017].

Vasagard J. and Dyer G, (21 October, 2016) *Chinese hackers targeted US aircraft carrier*. Available from https://www.ft.com/content/b03bc7f0-9745-11e6-a1dc-bdf38d484582. [Accessed 1 August 2017].

Zhen L., (1 August 2017) *Xi says no 'individual, political party or group' will be allowed to hurt China's territorial integrity*. Available from http://www.scmp.com/news/china/diplomacy-defence/article/2104901/xi-says-no-individual-political-party-or-group-will-be. [Accessed 1 August 2017].

Zetter K., (3 November 2014) *An unprecedented look at Stuxnet, the world's first digital weapon*. Available from https://www.wired.com/2014/11/countdown-to-zero-days-stuxnet/. [Accessed 7 February 2017].

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies