National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

HYBRID WARFARE: CHINA VS THE UNITED STATES AND THE WEST

By Lieutenant-Colonel Thinh Nguyen

JCSP 46

Solo Flight

Disclaimer

PCEMI 46

Solo Flight

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 - 2020

SOLO FLIGHT

HYBRID WARFARE: CHINA VS THE UNITED STATES AND THE WEST

By Lieutenant-Colonel Thinh Nguyen

Word Count: 5,396

Nombre de mots : 5.396

HYBRID WARFARE: CHINA VS THE UNITED STATES AND THE WEST

Introduction

Russia's annexation of Crimea shortly after it hosted the 2014 Winter Olympics in Sochi without a shot being fired took the world by surprise. In the same year, China started turning some reefs in the South China Sea (SCS) based into islands that is now home to military installations and a runway able to land large military aircraft. Both of these successful operations have since been characterized by western militaries and academia as a textbook cases of *hybrid warfare*, a term that has come to describe many activities below the threshold of war taken by Russia and China in the last ten years.

This paper will argue that China is conducting hybrid warfare against the United States (U.S.) and, by extension the West with the goal to destabilize the current international rules-based order and to gain more influence on the world state. To that end, Beijing is ready to resort to any mean that will provide it with an advantage. More specifically, this paper will show that China has conducted intellectual property (IP) theft warfare, legal warfare (lawfare), and financial warfare with great success to the detriment of the U.S. It will start with the definition of hybrid warfare to distinguish it from asymmetric warfare, and that hybrid warfare comprises multiple methods of operation. It will be followed with a little history of China's People Liberation Army (PLA) evolution since the mid-1980s to become a serious threat to the U.S. and West. Then it will proceed with linking China's activities in cyber espionage, the SCS, and global investment its hybrid warfare operations. The paper will conclude that it is not too late for the U.S. and the West to take actions to counter China's rise and influence despite some initial setbacks.

Definition

Though it has been prolific in recent years, what does *hybrid warfare* really means? From a strategy perspective, Jim Sciutto, author of *The Shadow War* and a former chief of staff at the U.S. Embassy in China, defines it as attacking an enemy "using a range of hard- and soft-power tactics: from cyberattacks on critical infrastructure, to deploying threats to space assets, to information operations designed to spark domestic division, to territorial acquisition just short of a formal invasion."[1] In other words, states (or non-state) actors are confronting each other without a formal declaration of war. They are in constant competition with one another, using both direct and indirect means.

Sergio Miracola, a researcher at the Italian Institute for International Political Studies, suggests that hybrid warfare distinguishes itself from asymmetric warfare "for the simple fact that it envisages the multiple, simultaneous use of different types of operational systems**,** which range from the conventional to the unconventional spectrum."[2] The unconventional spectrum is often referred in military parlance and in the spectrum of conflict as the "gray zone", an area that is becoming increasingly difficult to discern between peacetime and wartime operations with the advent of technology. From the Chinese perspective, the unconventional spectrum of hybrid warfare encompasses military, trans-military and non-military methods of operations. In *Unrestricted Warfare: China's Master Plan to Destroy America*, two former PLA's colonels, Qiao Liang and Wang Xiangsui, listed the following methods of operation that China and the PLA consider to be within the unconventional spectrum of warfare: atomic, diplomatic, financial, network, trade, bio-chemical, intelligence, resources, ecological, psychological, economic aid, space, regulatory, electronic, smuggling, sanction, guerrilla, drug, media, terrorist,

[1] Jim Sciutto, *The Shadow War: Inside Russia's and China's Secret Operations to Defeat America* (New York: HarperCollins, 2019), 11.
[2] Sergio Miracola, "Chinese Hybrid Warfare." *Italian Institute for International Political Studies*. 21 December 2018.

virtual, and ideological.[3] Surprisingly, not on their list are cyber and intellectual property theft. It may be justified that at time the book was written, 1999, these two terms were not prominent. It is worth noting that any of these methods can be used alone or in combination in an operation.

Hybrid warfare may be summarized as activities undertaking to *deceive the opponent to gain an advantage using whatever methods necessary, conventional or unconventional, military or non-military during all spectrum of conflict short of declaring war*. More emphasis is placed on non-military and soft power.

The PLA

In the mid-1980s the PLA started a slow transformation toward a more modern military force with emphasis on adopting technology and upgrading its equipment, training, education. Doctrinally, the PLA shifted focus from "People's war" – based on large scale total war – to "limited wars" or "local wars.[4] The PLA, whose primary existence is to serve and protect the Chinese Communist Party (CCP) – not the people - would become a more professional military, but still remain under the firm control of the CCP. The transformation was significant, both in term of the PLA's size and capability. Through three demobilizations and force reductions over the next twenty years, the PLA's size went from 4.5 million troops to 2.2 million by 2006.[5]

On capability, it is best described by Dr. Larry M. Wortzel, a leading authority on China and Asia, and a Colonel (retired) U.S. Army Intelligence Officer. He recalled attending a conference in 1988 on the PLA where an expert described the PLA as "a military that lacked the capability to be anything more than a nuisance…[and its] equipment was characterized as

---

[3] Liang Qiao and X. Wang, *Unrestricted Warfare: China's master plan to destroy America (*Panama City, Panama: Pan American Publishing Company, 2002), 123.
[4] Larry M. Wortzel, *The Dragon Extends Its Reach: Chinese military power goes global* (Washington, D.C.: Potomac Books, 2013), 22.
[5] Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, California: Praeger, 2017), 22.

obsolete, and its ability to operate beyond its borders was described as minimal."[6] Initial progress reforming the PLA was slow. However, almost twenty years later, Wortzel presented his own paper at a major conference on the PLA at the U.S. Army War College on China's advances in command, control, communications, computers, intelligence surveillance, and reconnaissance (C^4ISR). He argued that the PLA had come a long way and "had begun development of a major new ballistic missile variant that it thought could successfully attack a U.S. aircraft carrier with a maneuvering warhead."[7] A maneuvering warhead is significant leap in technology because traditional ballistic missiles, once launched cannot adjust it flight path to hit a maneuvering target. But the PLA's new *Dong Feng-21D* ballistic missile system is equipped with a guidance system that allows it to adjust its warhead up to one hundred kilometres upon reentry during the terminal phase of flight path making it an ideal weapon system against aircraft carriers.[8] Wortzel observed, the PLA has "modernized its equipment, focused on training its personnel, and changed its mission to meet the challenges of the new times."[9], the PLA realized the advance in weaponry and technologies had forever changed how future wars would be fought. The PLA concluded that future wars and conflict would be characterized by the "three nons": *noncontact, nonlinear, and nonsymmetric*.[10]

Noncontact refers to the replacement or reduction of close ground troops engagement thanks to long-range, precision strikes capabilities, extended-range artillery and rockets, long range bombers and submarines carrying cruise missiles that allow the engagement of adversaries well beyond visual range. *Nonlinear* refers to a lack of clear battle line that separates the two

[6] Larry M. Wortzel, *The Dragon Extends Its Reach:…*, ix.
[7] Larry M. Wortzel, *The Dragon Extends Its Reach*…, x.
[8] *Ibid*, 36.
[9] *Ibid*, x.
[10] Dean Cheng, *Cyber Dragon:...*, 25.

sides thanks to long reach of weapons there is no longer a distinct front or rear area. Furthermore, the emergent importance of information "means that the main battlefield in future wars will be in information space, with physical space [being] only one component."[11] *Nonsymmetric* refers to the Chinese's view of the West's asymmetric operations: the ability and capability to use airpower to counter land power such as strategic bombing campaign, surface and subsurface cruise missiles, and the substitution of close air support for ground-based artillery.[12] To meet this new challenge, the PLA set out to modernize its armed forces with the aim to not only become a regional power but also superpower. To achieve that goal, China needed to adopt new technology, and develop new and advanced weapons and weapon systems.

With the demise of the former Soviet Union, China saw the United States as the only superpower, one that it believes it will have to military confront one day. Wortzel observed "PLA military thinkers not only use the United States as the model for the force they must train to counter, but they also believe it poses China's most formidable potential adversary."[13] It is not a question of if, but when. As China's defense minister from 1993 to 2003, General Chi Haotian, was quoted saying "War [with the United States] is inevitable; we cannot avoid it. The issue is that the Chinese armed forces must control the initiative in this war…We must be prepared to fight for one year, two years, or even longer."[14] Although this was said about twenty years ago and in the context of the Taiwan dispute, with whom the U.S. has a defense agreement, it is not unthinkable that such conflict could occur given that Beijing still sees Taiwan a breakaway Chinese province that needs to return to its motherland.

---

[11] Dean Cheng, *Cyber Dragon:…*, 25.
[12] *Ibid.*
[13] Larry M. Wortzel, *The Dragon Extends Its Reach...*, 29.
[14] Liang Qiao and X. Wang, *Unrestricted Warfare…*, x.

Cyber Espionage Warfare

As part of the PLA's transformation plan, China encouraged the development of its own defense industry to lessen its reliance on foreign (most Russian) arms purchase. But Beijing understood that developing its own technology takes times and require large investment in research and development (R&D). To catch up with the West technologically, it has resorted to conducting cyber espionage warfare to steal intellectual property (IP) from western defence contractors. There is no better place to look than the U.S. The following is case of cyber espionage that helped China develop two weapon systems for its air force.

In 2014 China unveiled a full scale of its new, fifth generation stealth fighter, the J-31. Observers noticed a striking resemblance to the U.S. F-35. Two years later when the PLA Air Force first strategic transport aircraft, the Y-20, entered service, Jay Bennett of *Popular Mechanics* noted "the Y-20 is remarkably similar to the [USAF] C-17"[15]. As reported by Sciutto, it was no coincidence that these two Chinese aircraft resemble their U.S. counterparts: the aircraft's blueprints were stolen from the U.S. manufacturers. The same year that China unveiled its J-31, the U.S. Federal Bureau of Investigation (FBI) arrested and charged a Chinese businessman by the name of Stephen Su with IP theft after a lengthy investigation. In a plea deal for a reduced sentence, he admitted to having gained "unauthorized access to protected computer networks in the United States, including computers belonging to the Boeing Company in Orange County, California, to obtain sensitive military information and to export that information illegally from the United States to China."[16] What he was accused of stealing and how he did it comes straight out of China's playbook on industrial espionage.

[15] Jay Bennett, "China's New Y-20 Is the Largest Military Aircraft Currently in Production," Popular Mechanics, 20 June 2016.
[16] Jim Sciutto, *The Shadow War*:.., 55.

Su lived in China but frequently travelled to the U.S. and Canada for his small business manufacturing aircraft cable harnesses for the military aircraft sector. Although low tech product, he used his business to build contacts and establish a network inside some of the biggest defense contractors in the U.S., namely Lockheed-Martin and Boeing, manufacturers of the F-35 Lightning and C-17 Globemaster, respectively. Su was not a Chinese government employed hacker or spy in the traditional sense, but rather was an "independent contractor." According to the FBI indictment, he worked in a team with two other who were located in mainland China. Su's task to identify "targets" inside these companies, and then relay that information back to his co-conspirators in China who would carry out the cyber intrusion into the company's network. In one email in August 2009, he had attached an Excel sheet with names, email address, phone numbers and positions of eighty engineers and other personnel inside various defense contractors.[17] Su's team would then send a phishing email to employees of the target company. Once the recipient clicks on the attachment, an outbound connection would be established between the victim's computer and one in China under the hacker's control. In the case with Boeing, Su's team had "unfettered access inside Boeing's network for three years before the intrusion was first discovered. [They] claimed to have stolen 630,000 digital files-totaling a gargantuan 65 gigabytes of data on the C-17 alone."[18] These files were then be sold to Chinese state-owned aircraft manufacturers through intermediaries.

The discovery and arrest of Su's cyber theft was a success story for the FBI. However, that case was only the tip of the iceberg in term of cyber theft of IP and military technologies by China. According to Bob Anderson, the FBI's former head of counterintelligence, the FBI Cyber Division is only aware of 10 percent or less of all intrusions the like of the one carried out by Su

[17] Jim Sciutto, *The Shadow War:..*, 43.
[18] *Ibid*, 45.

and his team.[19] China has a vast army of hackers, both directly employed and contractors, dedicated to stealing America's most sensitive government and private sector secrets. The Office of the US Trade Representative estimate that the U.S. loses up to $600 billion annually in IP, and believes China is responsible for the bulk of those theft and losses.[20] While the U.S. may be its biggest, it is hardly the only target of Chinese's espionage. In a U.K. MI-5 (domestic counter-intelligence and security agency) 2010 report, it stated that China "represents one of the most significant espionage threats to the UK."[21] Canada's former director of Canadian Security Intelligence Service (CSIS) told a Senate committee in 2007 that "China accounts for close to 50 percent of our counterintelligence program."[22]

Investigating such a case takes years and a lot of resources that the FBI does not have enough. While the FBI celebrates the dismantling of this team and halted this particular theft, the damage has already been done. As Sciutto puts it, this theft has "allowed China to advance its military technology by years or more in the process. And today China is flying two jets that at least look almost exactly like the F-35 and C-17."[23] Not surprising, Beijing has denied any connection to Su and his team. To further conceal any possible connection to China, Su's team would download the data from a terminal in Hong Kong or Macao, and then hand carry the stolen data into mainland China.[24]

---

[19] Jim Sciutto, *The Shadow War:..,,* 57.
[20] *Ibid,* 45.
[21] William Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology acquisition and military modernization* (New York: Routledge, 2013), 187.
[22] *Ibid,* 188.
[23] Jim Sciutto, *The Shadow War:…*, 57.
[24] *Ibid,* 44.

South China Sea: Building Islands

In 2014 China started building islands in the in the contested Spratly Islands in the South China Sea (SCS), off the west coast of the Philippines. In less than 18 months, it has turned three reefs into fully fledged islands with military and civilian installations. At an estimated cost of five billion U.S. dollars, Beijing's claim on these reefs were based on *historic rights*.[25] Beijing's maneuvering on the international stage in regard to these islands building can be categorized as a case of lawfare.

Professor Iulian Chifu, a specialist in conflict analysis at the National Defence College, Bucharest (Romania), defines lawfare as "the use of law and judicial processes as an instrument of warfare, as a strategy of using (or misusing) the law instead of military actions or as complementary instrument to traditional military actions in order to achieve military objectives."[26] China's building of artificial islands in the South China Sea (SCS) is an example of the manipulation of international law to justify its action and achieve both its strategic and military objectives. As with any legal process, one can make a positive use the law for the protection of values, human right, and the accused. On the hand, a negative use of the law is defined as "misuse of the law, the abuse of provisions of the law or even twisting the sense and content of the law in order to achieve military objectives."[27] China has been taken advantage of the lack of clarity of certain international law and regulations to justify and defend its actions in the SCS.

China asserted the island building was in accordance with the United Nations Convention on the Law of the Sea (UNCLOS) Article 60. The Convention allows coastal states the right to build artificial islands within its exclusive economic zone, and shall retain exclusive jurisdiction

[25] Permanent Court of Arbitration, *Press Release: The South China Sea Arbitration* (The Hague: 12 July 2016).
[26] Greg Simons and I. Chifu, *The Changing Face of Warfare in the 21st Century (*New York: Routledge, 2018), 87.
[27] *Ibid.*

over such artificial islands.[28] Moreover, China pointed out that other countries have in the past built artificial islands. For example, the United Arab Emirates' *Palm Jumeirah* or Palm Islands built in the early 2000ss that house privates residences and hotels in Dubai. It also noted that Japan and Brazil have built artificial islands in the 1970s for their salts and coal industry with both being still in use today.[29]

With such precedence, one may ask what is the concern with the Chinese artificial islands in the SCS? Beijing's claim to the islands based on *historic rights* has no validity. In fact, the Philippines took China to the Permanent Court of Arbitration (PCA) in The Hague, which in 2016 issued "a sweeping rebuke of China's behaviour in the South China Sea, including its construction of artificial islands, and found that its expansive claim to sovereignty over the waters had no legal basis."[30] The ruling is binding as both China and the Philippines are signatories to the UNCLOS, but unfortunately, the PCA does not have enforcement power. Beijing had boycotted Beijing had boycotted the hearing process and ignored the ruling without any tangible consequences, economic, military, or otherwise.

The US is cognizant of the force projection the islands offer, and has publicly called on Beijing to adhere to the ruling. However, the U.S. has not taken concrete action to force Beijing to abandon these military outposts or at least discourage their further development. Since 2015, the US Navy has regularly (and with increasing frequency) conducted Freedom of Navigation Operations (FONOP) in the SCS by sailing near these new islands. And the US Air Force has conducted overflights both to document the development of the islands, and to ensure freedom of the airspace.

---

[28] United Nations General Assembly, *United Nations Convention on the Law of the Sea* (New York: UN, 1982), Article1 60.
[29] Simons, *The Changing Face of Warfare in the 21st Century*…104.
[30] *Ibid,*108.

China's continued occupation and control of these islands demonstrate its ability to use UNCLOS to sow some confusion on the world stage while it proceeded with building these artificial islands. By ignoring and international ruling, it has shown the region and the world that it is now a regional hegemony. Beijing has successfully used lawfare to achieve its strategic and military objectives without firing a shot.

Belt and Road Initiatives

Building on its growing economic strength, China is using its financial might as a leverage to gain favors around through so-called investments in infrastructures and energy projects in countries around the world. From a military perspective, it is using those investment as an expansion strategy for the PLA. This is *financial warfare*, which is the use financial system (money and credit)[31] against a country in order to weaken it or to compel it to change its policy or behaviour. It is distinct from economic warfare in that this latter uses trades boycotts, sanctions, and tariffs against the adversary. China is being very successful in this form of hybrid warfare.

In 2013, China's then new President Xi Jinping announced Beijing's ambitious plan for a global investment strategy called "One Belt, One Road" (subsequently called Belt and Road Initiative - BRI). BRI called for China to lead and provide the initial financing in the building of transportation and energy infrastructure and industrial parks on three continents: Asia, Europe, and Africa (it has since expanded to include projects in Central and South America and the Caribbean). Over the BRI's 35 years plan, the China Development Bank (CDB) estimated the funding required at U.S. $890 billion.[32] Beijing has publicly promoted the economic benefits of

[31] Paul Bracken, "Financial Warfare." *Foreign policy research institute*, 13 September 2007.
[32] Congressional Research Service, *China's "One Belt, One Road"*, (Washington, DC: U.S. Government Printing Office, 2015).

BRI for both China and its participants. There is some truth to this claim as a slowing Chinese economy and trades dispute with the U.S. have put pressure on the Chinese leadership to open new markets for its goods and services. Beijing sees BRI a "a way for China to develop new investment opportunities, cultivate export markets, and boost Chinese incomes and domestic consumption."[33]

From a geopolitical lens, BRI is a vehicle for Beijing to assert its influence outside of the South East Asian region. Elizabeth C. Economy from the Council on Foreign Relations, a Washington, DC-based think tank, wrote "Under Xi, China now actively seeks to shape international norms and institutions and forcefully asserts its presence on the global stage."[34] It is impressive that so far more than sixty countries – accounting for two-thirds of the world's population – have signed up or indicated an interest for BRI sponsored projects, and China has spent over US $200 billion.[35] However, critics argue that BRI is a debt trap for many countries.

Under the BRI umbrella, Beijing initially provides low interest loans (not aid grant) on the condition that Chinese firms are used as primary contractors. This arrangement has led to inflated costs, cancelled projects and backlash.[36] For example, in 2018 Malaysia elected Prime Minister Mahathir bin Mohamad who campaigned against over-priced BRI projects, and cancelled $22 billion worth of projects once in office.[37] However, about a year

[33] Andrew Chatzky and J. McBride, "China's Massive Belt and Road Initiative," *Council on foreign relations*. Last updated 28 January 2020.
[34] *Ibid*.
[35] *Ibid*.
[36] *Ibid*.
[37] *Ibid*.

later he gave his full support to BRI after a successful renegotiation and a 30 percent cut in the East Coast Rail Link project.[38]

Not all BRI participant states had the ability to renegotiate their projects for favourable terms as Malaysia. One such participant is Sri Lanka, which is heavily indebted to China, had to hand over control of its Hambantota Port for 99 years in a financing and debt relief deal. It all began in 2007 (pre-BRI) when, then Sri Lanka's President Rajapaksa called for the development of a port in his home district of Hambantota, about 250 km south east of Colombo. Many Sri Lankan officials questioned the wisdom of the project, especially when feasibilities studies concluded the new port would not be economically viable, and given that the main port in Colombo was thriving and had capacity for expansion. Ignoring the findings of the feasibilities studies, the President gave the green light to proceed with the development, however he could not find any private investor for its project. Sri Lanka turned to China which lent an initial $307 million from its Export-Import Bank with the conditions that Sri Lanka accepts China Harbor Engineering Company, one of Beijing's largest stated-owned enterprises, as its port's builder. This practice of sole source contracts to Chinese companies, who then bring in Chinese workers to perform the work, was a critical condition to obtain financing from Beijing.[39] Completed in 2010, the port is located on the sea route that sees tens of thousands of cargo ship transits, yet the port only saw 34 ships berthed in 2012, compared to 3667 ships that docked at the Colombo Port that year.[40]

Despite being a money losing operation, but wanting to take advantage of the BRI financing, President Rajapaksa instructed the Hambantota Port Authority to proceed with an

---

[3838] Kinling Lo, "Malaysia's Mahathir backs China's belt and road but insists on open trade routes," South China Morning Post, 26 April 2019.
[39] Maria Abi-Habib, "How China got Sri Lanka to Cough Up a Port," The New York Times, 25 June 2018.
[40] *Ibid.*

expansion of the port ten years ahead of the schedule as the initial plan called for expansion only once the port became profitable. To finance this Phase 2 of the development, Sri Lanka once again turned to China, this time for $757 million loan under the BRI umbrella.[41] Beijing agreed, but this time with higher rate, including the renegotiation of the initial loan to the new rate. The new loan and the higher rate put Sri Lanka in further debt toward China. By 2017, with some debt payments coming due, Sri Lanka was unable to service those debts and was forced to renegotiate with Beijing for new terms. Under this latest deal, China Merchant Ports (another state-owned company) would own 85 percent and the Sri Lankan Government 15 percent of new joint company to operate the port for a 99-year term. In addition, the new joint company will have control of 15,000 acres of land surrounding the port for future development of an "industrial zone".[42]

Although the deal prohibits the use of the port for any military purpose "without authorization" from the government in Colombo, critics argue that under pressure from China, the Sri Lankan government will allow PLA to establish a military post or installation in the future. Such military establishment would give the PLA a strategic position in the Indian Ocean, one that makes Indian military planners nervous.

Did China envision such a plan right from the start of the project? At least one person thought it did; the former Indian foreign secretary and national security advisor during the Hambantota Port project, Mr. Shivshankar Menon, once said of the project, "it was an economic dud then, and it's an economic dud now. The only way to justify the investment in Hambantota

[41] Maria Abi-Habib, "How China got Sri Lanka…
[42] *Ibid.*

is from a national security standpoint — that they [China] will bring the People's Liberation Army in."[43]

Sri Lanka is hardly alone to be indebted to China. Djibouti, the tiny East African country at the Horn of Africa has recently handed over operations of a container terminal, built with financing from BRI, to China Merchants Ports. China holds 71% of Djibouti's debt.[44] Djibouti is also home to China's first oversea military base, a naval support base, established in 2017.

While most of the BRI projects are aimed at developing countries, developed countries are welcomed to join. In March 2019, Italy shocked the G7 Alliance when it signed a Memorandum of Understanding (MOU) with China to partake in BRI. Although non-binding, the initial MOU call for 29 deals worth US $2.8 billion in investment in transportation, logistics, and port infrastructure in Italy.[45] Notable port cities in the deal are Genoa and Trieste will give China direct access to the broad European markets via existing rail links. In addition, it will give China access to third markets such as United States and Canada, via its European network. This deal marks the first major European economy and the first Group of Seven (G7) country to sign up to the Chinese global infrastructure and investment project.

From a geopolitical view, Italy's joining the BRI is a strategic windfall for Beijing at a time when European Union is trying to present a unified effort to counter Chinese influence on the continent. The bilateral deal gives Beijing a strong foothold in the heart of Europe. Critics argue that this deal is another debt trap for the already highly indebted country that will end with a similar fate as the Sri Lanka' Hambantota Port project or the Pakistan's Gwadar Port project

---

[43] *Ibid.*
[44] Max Bearak, "In strategic Djibouti, a microcosm of China's growing foothold in Africa," *The Washington Post,* 30 December 2019.
[45] Holly Ellyatt, "Is Italy playing with fire when it comes to China?", CNBC, 27 March 2019. https://www.cnbc.com/2019/03/27/italys-joins-chinas-belt-and-road-initiative.html

that ended up with the China Overseas Port Holding Company taking over operations when Pakistan was unable to pay back the debt.[46]

There is no doubt that through BRI investment, Beijing is "purchasing" its global influence one country at a time. For example, in 2017 Greece blocked a EU statement at the United Nations would have criticized China's human right records. Amnesty International and Human Rights Watch reported that was the first time the EU failed to make a statement at the UN right's body.[47] Coincidentally, a year earlier, Chinese state-owned China Ocean Shipping Company (COSCO) had invested and taken control of the Greece Port of Piraeus, Europe's largest passenger port with 20 million passengers annually.[48] The concession agreement which runs until 2052, followed a gradual investment in the port that started in 2010 and cumulated with a total of $1.9 billion investment that saw COSCO take over the operation of the container terminals, cruise ship piers, and ferry quays. While the Port of Piraeus is not a military port, in July 2017 three PLA Navy ships did a port call to Piraeus.[49]

Across the Atlantic, Beijing had been at hard at work in central America. In August 2018, El Salvador switched its diplomatic recognition from the Republic of China (Taiwan) to People's Republic of China. In doing so, El Salvador became the latest country to officially recognize Beijing as the legitimate Chinese government. El Salvador's switch of allegiance followed that of the Dominican Republic and Panama in recognizing Beijing in the previous two years. As reported by Douglas Farah and Caitlyn Yates from the National Defense University, three days after El Salvador announced the diplomatic recognition, the Chinese state-owned company Asia-

[46] Meziechi Nwogu, "China's Belt and Road Gets a Massive Victory in Italy," Goods and Services, 3 April 2019.
[47] Robin Emmott and A. Koutantou, "Greece blocks EU statement on China human rights at U.N.," Reuters, 18 June 2017.
[48] Meziechi Nwogu, "China's Belt…
[49] "Chinese Naval fleet arrives in Greece for a friendly visit," *ekathimerini.com*, 23 July 2017.

Pacific Xuanhao (APX) announced a proposal to lease 180 acres of land and to invest an initial $50 million within and around Puerto de la Union.[50] Once again, did China "purchase" this new diplomatic alliance? Evidence indicates that Chinese's investment did have an influence. Farah and Yates believe so when they stated "Such swift shifts are at least partially made possible by the PRC's ability to offer loans for major infrastructure projects, aid under the Belt and Road Initiative (BRI), and private investment from Chinese companies."[51] They also believe that investment in this El Salvador port has a strategic and military goal beyond just economics. They went on to say "Of greater concern is that the projects' scale masks true Chinese strategic and possible military interests in particular zones of the Western Hemisphere where such projects are currently under way."[52]

Observers of Chinese investment in El Salvador question the economic viability of some of these projects. For instance, a Japanese corporation conducted a feasibility study of the Puerto de la Union in 2014. The Japanese study confirmed the findings of separate studies since 1997 that concluded the Puerto de Union is not economically viable because its channel is too narrow and shallow for large ships. Recurring costly dredging will be required in order accept large ships, which makes the port economically non-viable.[53] Yet China's APX proceeded with a $50 million investment (with a potential for another $50 million). This strategy is a dejà-vu in Sri Lanka. If the Sri Lankan port is of any indication, El Salvador will not be able to repay the loan when its term come up, at which time the country will be forced to make deep concession such

[50] Douglas Farah and C. Yates, "El Salvador's Recognition of the People's Republic of China: A Regional Context" *Institute for National Strategic Studies, National Defense University* (Washington, D.C.: National Defense University Press, 2019), 18.
[51] Douglas Farah and C. Yates, "El Salvador's…, 3.
[52] *Ibid*.
[53] *Ibid*, 15.

as granting long term lease of the port and surround land to China with limited control of the port's operations.

China and its supporters call BRI an "efforts to reduce investment and trade barriers, such as customs procedures and the lack of a regional credit information system."[54] In 2015 President Obama commented on BRI "to the extent that China wants to put capital into development projects around the region, that's a positive."[55] He went on to insist for the "need for adherence to best practices, such as transparency about financing, and for projects to benefit local populations and not just 'the leaders of some countries and contractors.'"[56] The reality is that on most projects, China has sole sourced to one its own company and brought in Chinese workers to perform the work instead of hiring locals.

Conclusion

China's hybrid warfare goes by a different name: "winning without fighting" or "continuing competition" with the two sides being neither a pear or war. [57] In its quest to become a superpower, economically and military, China has resorted to hybrid warfare in order to level the playing with the U.S., whom it sees as its primary military foe. Its success in cyber espionage warfare and theft of industrial IP, and in particular defence IP, enabled China to develop new weapon systems in record time, saving years and millions in R&D while narrowing the military capability gap with U.S. Its tactic of using non-government employed hackers has allowed it to deny any involvement.

---

[54]Congressional Research Service, *South China Sea Disputes: Background and U.S. Policy* (Washington, DC: U.S. Government Printing Office, February 23, 2017).
[55] *Ibid.*
[56] *Ibid.*
[57] Jim Sciutto, *The Shadow War:…*, 13.

Beijing's attempt to use *lawfare* to justify its island building has failed to convince the PCA of the validity of its claim. However, its use of *lawfare* to achieve its strategic and military objectives in the SCS has succeeded. Beijing continues to occupy and build up military capability on these islands under the watchful eyes of the U.S. Its status as hegemon in the region and the lack of will power from the international community to enforce the PCA ruling, demonstrates Beijing's skillful navigation and misuse of lawfare to achieve its strategic and military objective without a shot being fired.

China's investment in ports in Asia and Africa should be concerning; in Europe it should worrisome; and in Central America it should be alarming. As the PLA Navy expand to become a blue water navy and project its power, it will be able to count on these ports for logistical support at worst. At best it may even setup additional military bases the like of Djibouti in Central America.

Though China has made great advances in its influence on the world stage and the PLA is fast closing the military gap with the U.S., the hybrid war is not lost. To counter the Chinese hybrid war, Sciutto proposes that the U.S. and by extension, the West take the following actions:

1. Know the enemy: China is a communist dictatorship;
2. Set red lines: make sure China knows it and does not cross;
3. Raise the costs: tailored retaliatory measures;
4. Bolster defenses: cyber and critical infrastructures;
5. Offense: credible offensive capability;
6. Warn of consequences: consequence of aggression;
7. New treaties for cyber and space: layout some basic rules;
8. Maintain and strengthen alliances: both military and international organizations; and

9. Leadership: leaders need to agree on common adversaries to focus effort.[58]

It is worth noting that many of the recommended actions require active participation and collaboration of stakeholders outside of the military. Combating a hybrid warfare requires a whole of government effort to include departments and agencies, as well as our allied partners.

This paper has presented three methods operation of hybrid warfare that China has conducted and is conducting with success. They are not the only one that China is employing successfully. Other methods operations that are actively employed by China are cyber, information, and space warfare. As such they are good subjects for another essay.

[58] Jim Sciutto, *The Shadow War:…*, 247-275.

BIBLIOGRAPHY

Bracken, Paul. "Financial Warfare." *Foreign policy research institute.* Last updated 13 September 2007. https://www.fpri.org/article/2007/09/financial-warfare/

Chatzky, Andrew and J. McBride. "China's Massive Belt and Road Initiative." *Council on foreign relations*. Last updated 28 January 2020. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

Cheng, Dean. *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*. Santa Barbara, California: Praeger, 2017.

Council on Foreign Relations. *Territorial Disputes in the South China Sea*. Last updated 26 March 2020. https://www.cfr.org/interactive/global-conflict-tracker/conflict/territorial-disputes-south-china-sea

Farah, Douglas, and Yates, C. "El Salvador's Recognition of the People's Republic of China: A Regional Context." *Institute for National Strategic Studies, National Defense University.* Washington, D.C.: National Defense University Press, 2019.

Hannas, William C., James Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology acquisition and military modernization*. New York: Routledge, 2013.

Mansoor, Peter R. "Introduction: Hybrid Warfare in History." In *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present,*1-17. New York: Cambridge University Press, 2012.

Mattis, Peter. "China's "Three Warfares" in Perspective." *War on the rocks.* 30 January 2018. https://warontherocks.com/2018/01/chinas-three-warfares-perspective/

Miracola, Sergio. "Chinese Hybrid Warfare." *Italian Institute for International Political Studies*. 21 December 2018. https://www.ispionline.it/en/pubblicazione/chinese-hybrid-warfare-21853

Permanent Court of Arbitration. *Press Release: The South China Sea Arbitration*. The Hague: 12 July 2016.

Qiao, Liang (Col), and (Col) X. Wang. *Unrestricted Warfare: China's master plan to destroy America.* Panama City, Panama: Pan American Publishing Company, 2002.

Sciutto, Jim. *The Shadow War: Inside Russia's and China's Secret Operations to Defeat America.* New York: HarperCollins, 2019.

Simons, Greg, and I. Chifu. *The Changing Face of Warfare in the 21st Century.* New York: Routledge, 2018.

United Nations General Assembly, *United Nations Convention on the Law of the Sea*, New York: UN, 1982.

United States. Congressional Research Service. *South China Sea Disputes: Background and U.S. Policy*. Washington, DC: U.S. Government Printing Office, February 23, 2017.

United States. Congressional Research Service. *China's "One Belt, One Road"*. Washington, DC: U.S. Government Printing Office, 6 August 2015.

Wortzel, Larry M. *The Dragon Extends Its Reach: Chinese military power goes global.* Washington, D.C.: Potomac Books, 2013.