Issues & Studies: A Social Science Quarterly on China, Taiwan,
and East Asian Affairs
Vol. 56, No. 3 (September 2020) 2040013 (29 pages)

DOI: 10.1142/S1013251120400135

The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea

Mark Bryan Manantan

This paper investigates the increasing use of cyber coercion by the People's Republic of China (PRC) among its core interests: Taiwan, Hong Kong, and the South China Sea. It argues that the PRC's deployment of sophisticated attacks in the form of cyber coercion continues to be part of its geostrategic playbook to exert its influence and prosecute its wider interests as a rising power in the Indo-Pacific region. However, it observes that cyber coercion will be employed by the PRC in concert with all the other tools — diplomatic, economic, and the political — across the spectrum. The paper has two broad goals: first to unpack the trends or patterns in the PRC-sponsored cyber coercion by accentuating contextual and operational dimensions using Taiwan, Hong Kong, and the South China Sea as analytical case studies; second, to highlight the opportunities and limitations of using cyber coercion as an asymmetrical capability in the changing threat landscape. The paper concludes that the PRC's cyber coercion is characterized by blurring the distinction on what constitutes compellence and deterrence. The boundaries are not clear cut, and to a certain degree both are even mutually reinforcing. The in-depth analysis of the case studies reveals the growing prominence of disinformation campaigns in close coordination with cyber operations (malware, phishing, and DDoS attack). This emboldens the PRC with a myriad of coercive strategies in shaping its external environment and realizing its ambition of national rejuvenation across Taiwan, Hong Kong, and the South China Sea.

Keywords: PRC; cyber coercion; cybersecurity; Taiwan; Hong Kong; South China Sea.

* * *

Mark Bryan Manantan is currently the Lilian and Lloyd Vasey Fellow at the Pacific Forum and a non-resident fellow at the Center for Southeast Asian Studies, National Chengchi University in Taipei. He was a visiting fellow at the East-West Center in Washington D.C. and the Center for Rule-making Strategies at Tama University in Tokyo, Japan as a US-Japan-Southeast Asia Partnership in a Dynamic Asia Fellow. He is also the Founder and Strategic Director of Bryman Media. He can be reached at <brymanmedia@gmail.com>.

In the lead-up to Taiwan's highly anticipated January 2020 presidential and legislative elections, the self-governing island is preparing for unprecedented cyberattacks from Mainland China (Spencer, 2019). Such a forecast on the possible surge of cyberattacks stems from previous incidents of reported hacking by a state-sponsored group based in China known as APT16 during the 2016 elections. The group launched cyberattacks which targeted local news organizations and the Democratic Progressive Party (DPP) to acquire information on policies and relevant documents (Bloomberg, 2015). Similarly, as the Hong Kong Protest against the controversial Anti-extradition bill ramps up, the People's Republic of China (PRC)-backed cyber operations were detected by Twitter (Twitter Safety, 2019). Datasets of anomalous activities of 936 fake accounts were publicly released (Uren, Thomas, & Wallis, 2019). The ultimate aim is to sow political discord and distract the social movement and collective protest. In 2016 at the height of the territorial disputes in the South China Sea, Chinese hackers targeted the communication systems of Vietnamese airports and used offensive language against the Philippines and Vietnam (Osborne, 2016). In a similar fashion, it was reported that the Philippines and China were embroiled in a "mutual cyber conflict" in 2012 following the stand-off in the Scarborough Shoal and Spratly Islands (Manantan, 2019b).

These scenarios demonstrate the increasing use of cyber-enabled operations of the PRC toward its core interests: Taiwan, Hong Kong, and the South China Sea. This paper aims to investigate such phenomena by asking, why does the PRC continue to employ cyber coercion at such an unprecedented scale? It is also critical to examine how the PRC employs cyber coercion.

In probing these questions, the study takes a deeper dive in analyzing the PRC's consolidation of its defense and security posture that is mainly driven by its position as a rising power. Contrary to the one-dimensional emphasis on China's heavy spending to upgrade its traditional defense arsenal, a more nuanced analysis reveals that Beijing is actually pursuing a two-pronged approach. On one hand, there is the obvious build up on China's defense spending across the spectrum from its Army to its Navy and Air Force. Amidst its growing allocation on traditional defense budget, however, China continues to invest in its hybrid warfare capabilities (Chase & Chan, 2016, p. 26). Despite its newfound military strength and rising power status that puts it in close range with the US, China continues to value asymmetric and gray-zone capabilities especially in the realm of its cyber operations to achieve its strategic objectives. Given these observations, this study endeavors to shed light on the emerging traction of cyber coercion in the context of Chinese-linked cyber operations. It builds on the previous

scholarly works on cyber coercion and its rising prominence in the literature of hybrid warfare (Hodgson, Ma, Marcinek, & Schwindt, 2019; Valeriano & Maness, 2014).

The paper argues that the PRC's cyber coercion in the form of sophisticated cyberattacks is an integral component of its geostrategic arsenal to exert its influence and prosecute its wider interests as a rising power fueled by its ambition for national rejuvenation. Cyber coercion perfectly captures China's strategic doctrine which blurs the notion of war or peacetime underpinned by its ideological clash with the Western liberal democracies. PRC-linked cyber coercion generally covers a wide range of operations — espionage, infiltration, data breach or theft, and distributed denial-of-service (DDoS) and disinformation campaigns — to advance China's interests without igniting an outright conflict against an adversary. However, it observes that cyber coercion will be employed in concert with all the other tools — diplomatic, economic, and the political — across the spectrum. The paper has two broad goals: first to unpack the distinct nature and depth of PRC-sponsored cyber coercion by accentuating operational and contextual dimensions to uncover the trends and patterns of cyber coercion using Taiwan, Hong Kong, and the South China Sea as analytical cases; second, it will also shed light on the opportunities and limitations of using cyber coercion as an asymmetrical capability in the evolving threat environment in international politics.

The entire paper unfolds as follows: following this introductory section, it will proceed to further discuss the conceptual dimension of cyber coercion and its strategic merits to achieving political gains in the rapidly changing terrain of international politics. It then analyzes the conception of cyber coercion in the context of the PRC. Recognizing that China is not the only active player in using cyber coercion, unpacking the assumptions that drive its indispensability from the perspective of the Chinese Communist Party or CCP is essential to understanding the goals and objectives of its implementation. The paper then moves to analyze the triumvirate of its case studies to identify, demonstrate, and analyze the deployment and impact of cyber coercion given the current geostrategic climate that underpins China's interests in the case subjects. Taiwan, Hong Kong, and the South China Sea were a major theater for the PRC's cyber operations, especially during the heightened political, economic, and diplomatic contestation. The examination of three interrelated cases will reveal subtle differences as well as similarities that will be critical to draw any pattern or trend toward the PRC's coercive behavior in the cyber domain. This section will also pay close attention to the interventions undertaken by non-state actors, particularly tech giants such as Facebook, Twitter, and Telegram, to counter Chinese-linked cyber coercion. The last section offers concluding remarks.

Defining Cyber Coercion

Cyber coercion is defined as the "threat (implied or explicit) or limited use of cyber operations to motivate a change in behavior by another actor that may involve cyber operations on their own or in conjunction with other coercive actions" (Hodgson et al., 2019, p. 7). In discussing the concept of cyber coercion, Schelling's (1966) seminal work on *Arms and Influence* is a fundamental starting point. Schelling identifies the two components of coercion: active coercion or compellence refers to the actual use of force to compel action whereas passive coercion or deterrence is the "threatened use of force to either motivate action or refrain from a particular action" (Hodgson et al., 2019, p. 5).

Active coercion or compellence requires a demonstration of commitment from the coercer to inflict some form or degree of pain or punishment to influence the coerced to change its behavior and forestall further consequences. There is a signaling aspect from the coercing state that puts the burden toward the threatened state to submit to its demands (Schelling, 1966). Applied in cyber coercion, compellence requires the deployment of threats to use force or the limited use of force (Fleming & Rowe, 2015). This gives the threatened actor/state an impression of the sufficient capabilities of the coercing state that might influence his/its course of action.

Passive coercion or deterrence is often conducted covertly to wreak punishment or pain against the threatened state, but the desired behavior or objective of the coercing state is vague. Since deterrence in cyber coercion operates within a certain degree of secrecy, the threat becomes ill-defined. It is challenging for a nation to deter by threatening to use cyber capabilities because it runs the risk of exposing the technical details of them, which could reduce the impact or effectiveness of the attack (Fleming & Rowe, 2015, p. 96). This could result in the threatened state mitigating any vulnerabilities within its system, which could reduce the impact or effectiveness of the attack from the coercing state (Fleming & Rowe, 2015, p. 96). To a certain degree, the covert execution of deterrence even discombobulates the clarity of the desired outcomes by the coercing state, thus failing to prevent the actions or illicit a favorable response from the threatened state. That is why cyber deterrence would often be used in coordination with other tools — political, military, and economic — (Valeriano, Jensen, & Maness, 2018) along with the use of proxies to convey a threat or make a clear demand (Hodgson et al., 2019).

The deployment of cyber coercion is quite complex given the possible "mixed signals" from the coercing state and the mismatch in the corresponding responses or an absent response on the part of the threatened actor. While the coercing state may be

using coercion as part of its larger strategic campaign or simply as an independent form of cyber operation, the threatened actor can assume that either or both are the case. The threatened actor would then choose to bolster its defenses or simply ignore it all with the assumption that state and non-state actors often infiltrate or intrude into computer networks and systems (Hodgson et al., 2019, p. 7).

Given this nature of cyber coercion, the views on its success or failure have been debated. As a general approach, the cost–benefit analysis has been adopted to determine whether a cyber operation has succeeded or failed based on weighing in the perceived costs and benefits of resisting or subjecting to the demands of the coercing state. The level of destabilizing costs that coercive measures can impose upon the threatened actor could lead to the capitulation and submission to the demands of the coercing state (Sharp, 2017), but other perspectives are more nuanced. Some doubt the punitive effects of cyber coercion and claim that it only forces the threatened actor to increase its defenses against potential attacks (Gartzke, 2013). In most instances, it often results in resistance over compliance, which fails to achieve the desired alternative courses of action (Gomez, 2018).

Recognizing the emerging debates on the continuing relevance of cyber coercion, this paper asserts that it will remain a critical tool in the strategic arsenal of competing states as the world becomes increasingly networked and interconnected. Compared to the constraints of launching kinetic attacks, cyber coercion provides a multitude of possibilities (R. A. Clarke & Knake, 2010). It can achieve "offense in depth" by offering a wide range of tactics and procedures (Fleming & Rowe, 2015).

As discussed, cyber coercion could involve the imposition of the actual threat or the threatened use of force against the target. Threats inject fear or doubt against the target state/actor, making it a vital tool in conducting psychological types of warfare. Exploiting vulnerabilities could force an adversary to recalibrate its actions or even capitulate. The use of a threat can establish the coercing state's commitment and inherent capabilities to infiltrate or gain access against its target's networks and systems (Neuman & Poznansky, 2016). It sets the tempo for the possibility of further escalation if the threatened actor does not submit to the desires of the coercing state. Such a threat if executed with utmost *resolve* and its potential to inflict further *damage* fundamentally carry strategic leverage (Neuman & Poznansky, 2016). There is no need for the coercer to specifically state its actions or intentions to be credible because the very act of exploiting one's vulnerability already depicts its capability to inflict or cause further harm, regardless of whether the target further raises its defenses.

The threat of the use of force in cyber coercion threads a delicate balance to avoid escalation. The coercer takes calculated steps in using deterrence to avoid certain risks

which could lead to capability loss or even spiral into destruction or escalation (Jensen, 2019). As instruments of covert operations, cyber capabilities appear less obvious compared to other strategic weapons (Lewis, 2011). The strategic currency fundamentally lies in achieving the "intelligence gain or loss dilemma" through low-level yet persistent intrusions against the computer systems and networks of an adversary (Jensen, 2019). Despite the prolonged period of intrusions, cyberattacks have a higher threshold to provoke military retaliation which does not ignite any kinetic action (Waxman, 2013). This is highly favorable on the part of the coercing state to achieve its strategic goals without igniting an outright war.

The essence of the cyber landscape where secrecy and covert operations abound positions cyber coercion as an indispensable gray-zone strategy tool which falls below the threshold of traditional armed conflict. Cyber coercion allows states and non-state actors to achieve their strategic objectives or exert political influence without resulting in a full-blown confrontation (Fleming & Rowe, 2015). Viewed from the lens of hybrid warfare, cyber coercion is an asymmetric approach that aims to achieve consequences using different means at varying intensities (Danyk, Maliarchuk, & Briggs, 2017). Moreover, it not only does exploit vulnerabilities in critical infrastructures but also leverages the prevailing socio-political and economic climate to launch disinformation campaigns via social media against its target. Therefore, cyber coercion can exploit all types of vulnerabilities in software, hardware, and human society. It is so highly fluid that it can integrate or combine characteristics of both compellence and deterrence. It can also capitalize on susceptible points to achieve strategic goals without the use of conventional military force.

With this growing evidence on the nature, depth, and merits of cyber coercion, this paper's primary focus shifts from questioning its strategic value toward providing a more nuanced and practical understanding of its conception and application. It aims to highlight two critical dimensions — contextual and operational — to provide insights that better explicate the trends and patterns which underpin its emergence and impact when conducted by a particular state or non-state actor. Applied in the analysis of the PRC's cyber coercion, the contextual dimension pertains to the prevailing landscape or atmosphere in international affairs when the act of cyber coercion is employed. It refers to the increasing competition or heightened political interactions among states and non-state actors with respect to a particular foreign policy and/or the geopolitical issue(s) between the PRC and the three analytical case studies. At the same time the reference to the operational dimension shall cover the specific methods of cyber coercion from malware, data leaks, phishing emails, and disinformation campaigns. It will also highlight specific technical items such as exploits, tactics,

techniques, and procedures (TTPs) that are unique to a specific group of hackers. The operational dimension will emphasize how specific incidents are linked to a suspected state or non-state actor(s) that are made available through published and open-source materials like white papers and new articles.

In accentuating the contextual and operational dimensions of cyber coercion, the paper shall refer to the "compellence or deterrence" framework conceived by Fleming and Rowe (2015) to examine deployment and intended effects of coercion in the cyber domain. It provides a broader analytical lens that will illuminate the nuances of cyber coercion tactics which are characterized as fluid and at times mutually reinforcing.

Understanding China's Cyber Coercion

The fundamental guiding principle behind China's use of cyber operations more broadly is rooted in its concept of "omnipresent struggle" where there is no distinction between peace or wartime and the front line or home front (Hodgson et al., 2019, p. 16). This captures China's view of military competition that centers on the enduring conflict between political systems and ideologies (Chase & Chan, 2016, p. 26). It echoes the PRC's strategic imperative to dominate the cyber realm and conduct a new form of hybrid warfare that uses cyber forces to win information-based battles (Kolton, 2017). According to *The Science of Military Strategy* published in 2013, the People's Liberation Army or PLA asserts that cyberspace has become a new ground for contestation where states have begun to vie for information security during peacetime while simultaneously striving to gain network dominance against their rivals in the event that a major conflict erupts. It must continuously develop both its defensive and offensive capabilities in conducting information warfare and deterring large-scale information attacks (Shou, 2013). The same document articulated the need to expand China's strategic defense posture through its network warfare capabilities (Shou, 2013).

The PLA uses "network operations" to capture the broad concept of information conflict, which is the closest term to the US doctrinal term of cyberspace operations (Hodgson et al., 2019, p. 15). There are three categories of PLA cyber or network operations against an adversary's system or network: (i) network reconnaissance aims to gather information and expose the adversary's vulnerability; (ii) network attack and defense operations seek to inflict damage to the functional units of the adversary while protecting its own network; and (iii) network deterrence refers to the offensive and

defensive cyber capabilities of the PLA which aims to dissuade adversaries from attempting to launch attacks (Hodgson et al., 2019, pp. 15–16). The National Military Strategy released in 2015 crystallized the role of cybersecurity to protect and promote China's economic, social, and national security as the stakes for competition rise with the investment of other countries in cyber military forces. Hence, as part of its integrated strategic deterrence, the PLA can deploy these network capabilities to conduct espionage or paralyze an adversary's capacity to respond by launching cyberattacks (Hodgson et al., 2019, pp. 15–16). It can also implement such network warfare capabilities in close coordination with conventional strikes to deny its adversaries access to computer networks and information systems.

The Chinese term *weishe* (威摄), which translates to "deterrence" in English, closely captures the salient qualities of both deterrence and compellence previously discussed (Cheng, 2011). According to *The Science of Military Strategy 2005*, *weishe* works by either persuading the opponent to submit to the coercer's demands or preventing the opponent from engaging in anything that could have detrimental costs to the coercer. Hence, *weishe* can be a rough equivalent to Schelling's notion of coercion. The PLA considers *weishe* to be a centerpiece of its strategic thinking. Applying *weishe* in the context of network operations, the use of cyber capabilities provides the PLA with a unique form of leverage as an asymmetric response to an adversary or to defeat its enemies without waging a war. It can "sow fear and panic amongst the enemy" and "compel adversaries from rash activities" (Hodgson et al., 2019, p. 18).

The PRC undertakes "calculated" steps that surround its cyber coercion activities to achieve its desired objectives. It employs sophisticated precision in pursuing its targets to add credibility to its threats or actions. This is followed by a series of propaganda activities pre- and post-cyber operations to further ensure that the PRC's target is aware of its resolve to employ its cyber capabilities (Kolton, 2017, p. 135). Such propaganda may come from strong rhetoric or statements from Beijing or be funneled through Chinese state-owned media companies. It could also be in conjuncture with Beijing's use of its political, diplomatic, and economic leverage against the coerced state. These mechanisms thus demonstrate the PRC's commitment to ensure that the signaling efforts can be recognized by the threatened state.

China employs both military and civilian entities or proxies to launch its cyber operations. The primary government units responsible in cyber operations are the PLA and the Ministry of State Security. A report published by Mandiant in 2013 identified the 3rd General Service Department (GSD) and the 2nd Bureau to be responsible in carrying out the PLA's cyber operations (McWhorter, 2013). In the reshuffling of the

PLA in 2015, cyber operations along with space, electronic warfare, and psychological warfare were reassigned to the Strategic Support Force (SSF) (Costelo & McReynolds, 2018). Specifically, the SSF's Network Systems Department is tasked to oversee the overall cyber operations and to manage psychological and kinetic operations (Costelo & McReynolds, 2018).

Several Advanced Persistent Threat (APT) groups have been attributed to China over the past few years. Since 2013, the US cybersecurity firm FireEye has attributed 10 APT groups to China (FireEye, 2019). In 2014, PLA officers were indicted by the United States Department of Justice for the pilferage of trade secrets from Westinghouse, U.S. Steel, and other companies (Segal, 2018). In November 2017, three Chinese nationals linked to the Chinese cybersecurity firm Boyusec were charged with hacking various companies for commercial and financial gains (Segal, 2018). In December 2018, two Chinese hackers believed to be associated with the APT10 group under the Ministry of State Security were indicted due to cyber theft of intellectual property and business information (Office of Public Affairs, 2018). Nonetheless, not all groups were tied directly to the Chinese government, and some were also found to be working as private cyber groups that had been hired by the PRC (Groll, 2017).

The PLA also underscores the limitations of *weishe*. In parallel to the prevailing literature on the effectiveness of cyber coercion, the possible impact of *weishe* is also questionable. It poses significant risks of inadvertent escalation on the part of the coerced, and it could also have spill-over effects in other domains such as critical national infrastructures. Nonetheless, the PLA believes that intruding into a rival state's network still carries a coercive purpose. The idea of stealing data largely focused in information-gathering for intelligence purposes or undermining critics through disinformation campaigns has strategic value (Wang, 2007). For instance, network reconnaissance which exposes the vulnerabilities of the threatened actor could persuade it to undertake actions favorable to the coercing state. Network attack and defense operations also demonstrate a strong commitment from the PRC to further damage or exploit the adversary's systems. At the same time, network deterrence illustrates the PRC's resolve to raise the level of intrusions or damage if the adversary does not capitulate to its desires. These three categories of the PLA's cyber operations provide it with the strategic leverage to launch a pre-emptive strategy or response or shape its external environment and achieve its desired goals. It underscores how *weishe* combines the ideas of compellence and deterrence. In the proceeding analytical section of this paper, the term coercion will be adopted to refer to the Chinese-linked *weishe* (威摄) to demonstrate the blurring and/or integration of compellence and deterrence by the PRC and its proxies.

Demonstrating PRC's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea

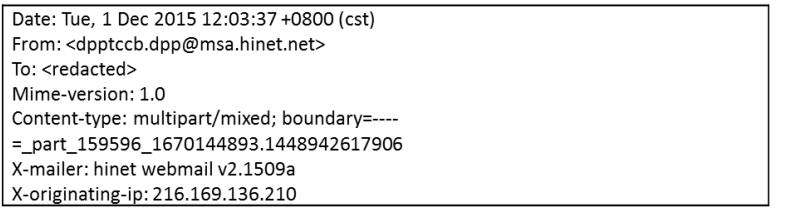
It can be argued that the integration of *weishe* by the PLA within its cyber operations is central to its strategy of pursuing the Chinese dream of reunification with Taiwan, tightening its political control in Hong Kong, and its assertion of its sovereignty in the South China Sea. This section shall look into each of these case studies and shall attempt to draw emerging trends, patterns, or variations in the deployment of cyber operations by the PRC to coerce or compete without igniting outright confrontation and paying particular attention to the proposed contextual and operational dimensions.

Taiwan's Presidential Elections 2020

It has become common knowledge that Taiwan is a laboratory for the PRC's cyber capabilities before they are deployed against rival states like the United States (Gold, 2013). Taiwan considers cyberattacks from the PRC as cost-effective measures to propagate a dystopian vision of the self-governing island's future, especially under the leadership of left-leaning President Tsai Ing-wen of the DPP (Spencer, 2019).

In the months leading up to Taiwan's highly anticipated 2020 presidential election, China's cyber coercion reached an unprecedented level of approximately 10–40 million attacks per month (Spencer, 2018; Yu, 2018). Such findings increase Taiwan's vulnerability from its national critical infrastructure to massive fake news and disinformation campaigns involving Chinese-backed hackers (Spencer, 2019). Taiwanese authorities have argued that detecting Chinese-linked cyber intrusions has also become even more challenging in recent times (Spencer, 2019). Suspected Chinese cyber hackers are using search engines such as Google and blogs to break into core systems and tamper information.

Aside from the increasing volume of cyberattacks, it is noteworthy to underscore the sophisticated approach of such operations. In 2015, the ruling DPP was the primary target of the Chinese-state-backed group APT16. The group was suspected to have infiltrated the DPP's staff emails and security protocols, spoofed account holders, and delivered malicious codes to conduct intelligence-gathering (Winters, 2015). As shown in Figure 1, other attacks were also sophisticated and targeted in nature: phishing emails were sent to key individuals belonging to academia and non-governmental organizations that supported the DPP's standing policy on Taiwan's *de facto* independence (Bloomberg, 2015).



Source: From Winters (2015).

Figure 1. A spear-phishing attack launched by APT16, a China-based hacking group, appearing to be a legitimate email from the DPP which targeted Taiwanese media organizations.

In addition to cyber intrusions and phishing emails, China has also upped the ante to complement its cyber coercion activities with information warfare using traditional and digital media platforms. The selection of the Kuomintang Party's standard bearer and former Kaohsiung Mayor Han Kuo-Yu evinced the mainland's use of social media manipulation led by a professional cyber group. Based on the forensics obtained, the social media accounts have IP addresses that can be traced back to China (Huang, 2019). According to the Taiwan Public Opinion Center, the meteoritic rise of Han is credited to his consistent community engagements in social media. Han boasts an unofficial Facebook fan page with 88,000 members to date (Huang, 2019). These die-hard fans generated likes, shares, and comments and propelled fake news and/or disinformation against Han's opponent in the primary (Huang, 2019). Such malicious content has often been shared on Line, a messaging app popular among Taiwanese.

China's political interference also involved in the so-called "red media" in charge of influencing popular sentiment in favor of China-friendly presidentiable candidates (Lee, 2019). Taiwan's National Security Bureau has tagged several Taiwanese media outfits cooperating with the CCP's Taiwan Affairs Office, including the prominent Want Want China Times Media Group (Kurlantzick, 2019).

China's coercion toward the ruling DPP party extends beyond the cyber domain. The massive attacks were complemented by Beijing's strong rhetoric against the self-ruled island. To add further credibility to its resolve to coerce Taiwan, Beijing used its massive political, economic, and diplomatic resources to achieve this objective. Since 2016, China has boycotted high-level interactions with the current left-leaning DPP-led government and diminished the flow of tourists from the mainland.

During the 40th anniversary of the so-called Message to Compatriots in Taiwan, Xi Jinping warned those who advocate for Taiwan's independence, declaring that the use of force remains a viable option for China to achieve reunification (Manantan, 2019a). But in the Tsai administration's pushback against China's one country, two

systems approach — marked by its increasing diplomatic engagements with Japan and talks of possible arms sales worth US$2.2 billion with the United States — Beijing's rhetoric and actions have also escalated (Ihara, 2019; "US Approves," 2019). It vowed to eliminate all of Taiwan's diplomatic allies if President Tsai is re-elected in 2020 (Zheng, 2019). To illustrate its commitment, Beijing lured the Solomon Islands and Kiribati with economic enticements to switch ties to Beijing. Taiwan lost the two Pacific islands just within a span of a week, leaving it with 15 countries with which it has formal relations (Zheng, 2019).

The Hong Kong Protest

In February 2019, the Hong Kong Security Bureau proposed the Fugitive Offenders Ordinance, a series of legislative amendments to Hong Kong's extradition laws which would allow criminal suspects to be sent to Mainland China for trial (Torde, 2019). Hong Kong residents argued that such legislation would provide the CCP with the legal instruments to prosecute individuals who express dissent against it (Mayberry, 2019). It would also put foreigners visiting or working in Hong Kong at the risk of being arrested if any suspicion were directed against them. Amidst the withdrawal of the controversial bill by the Hong Kong parliament in September 2019, the weekly protests became an everyday occurrence and morphed into violent clashes prompted by the Hong Kong Police Force against protesters ("Timeline: Key Dates," 2019).

As the protests intensified, Chinese-linked hackers targeted Telegram, the messaging platform used by the organizers. Compared to other messaging applications like WhatsApp, Telegram has standard end-to-end encryption that makes it less susceptible to spying or hacking (Shanapinda, 2019). However, spyware is not the only viable tool to infiltrate or disrupt the app. In June 2019, Telegram suffered a DDoS attack during the protests. Telegram servers were flooded with junk communications at 200–400 gigabits per second which caused its servers to malfunction (Shieber, 2019). The attack has also affected Telegram's 200 million users across the US and other countries. The DDoS attacks used botnets which were intended to take Telegram's service offline by flooding it with malicious types of communication and rendering it inaccessible. As illustrated in a tweet on Figure 2, Telegram confirmed that the IP addresses responsible in launching the DDoS attacks were attributed to China, and this coincided with the intensifying protests in Hong Kong (O'Flaherty, 2019). It was observed that the PRC's deployment of cyber-enabled operations was consistent with Beijing's tactical response to impose control against defiant groups that can imperil social order and the economy of Hong Kong (Mozur & Stevenson, 2019).

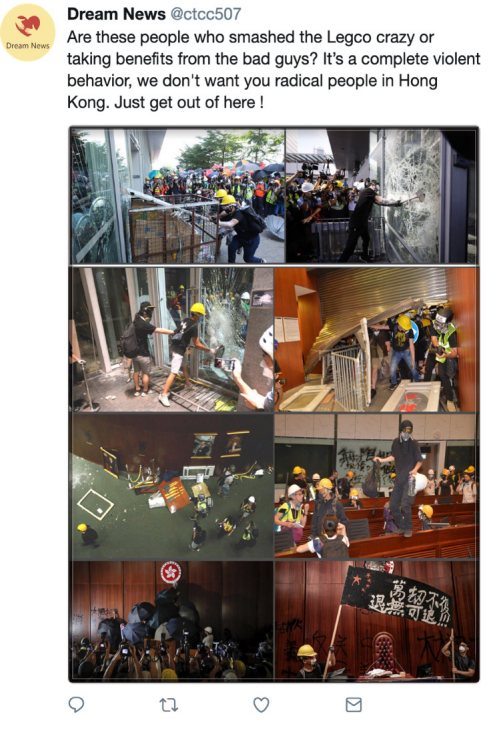
Source: From Kumar (2019).

Figure 2. Telegram founder Pavel Durov confirms the DDoS attack originated from IP addresses based in China to sabotage Hong Kong protesters.

In addition to disrupting Telegram, Ivan Ip, one of the administrators of the 30,000-member Telegram chat group, was also arrested by authorities on grounds of committing a public nuisance (Mozur & Stevenson, 2019). After crippling Telegram's service, protesters were forced to use highly vulnerable messaging platforms. This gave China greater surveillance capacity against individuals and groups that could be charged with conspiracy or prosecuted by their political actions (Shanapinda, 2019).

In August 2019, social media giants such as Facebook and Twitter suspended accounts that were linked to Chinese disinformation campaign groups aimed at discrediting Hong Kong protesters. Google-owned YouTube followed suit by banning 210 channels that resembled similar patterns of disinformation (Wood, McMinn, & Feng, 2019). Through its official blog, Twitter has revealed massive "coordinated state-backed" information operations that specifically focused on the political situation in Hong Kong (Twitter Safety, 2019). It identified 936 accounts that originated from Mainland China which attempted to sow political discord. Twitter claimed that the suspended accounts demonstrated "covert and manipulative behaviors (spam, coordinated activities, fake accounts, attributed activities, and ban evasion)" which violated its platform manipulation policies (Twitter Safety, 2019). Twitter has also announced that it will not accept any advertising from "state-controlled news media entities" (Twitter, Inc., 2019).

As described in Figure 3, it was observed that some of the accounts identified by Twitter had been previously used to target political opponents of the CCP as early as April 2017 (Twitter, Inc., 2019). Thus, it can be surmised that Chinese-linked covert information has been operating in social media platforms in the last two years. Such accounts were either repurposed spam accounts or marketing accounts with a sizeable number of followers, thus confirming the campaign's urgency to acquire credible



Source: From Twitter Safety (2019).

Figure 3. An account suspended by Twitter for violating its platform manipulation policies.

digital assets in a very short span of time as the protests intensified (Uren et al., 2019). An assessment of the tweets revealed that the main narratives focused on the "condemnation of protestors; support for the Hong Kong Police and the 'rule of law'; and conspiracy theorist about Western involvement in the protests" (Uren et al., 2019). Furthermore, the deliberate use of the Chinese language was also devised to influence Hong Kongers and the overseas Chinese diaspora (Uren et al., 2019).

Facebook, meanwhile, has also taken down seven pages, three groups, and five accounts that exhibited coordinated inauthentic behavior. The group was tracked to be located in China and had been working against the ongoing protests in Hong Kong (Gleicher, 2019). Following the information provided by Twitter, Facebook conducted its own internal investigation and confirmed a similar "coordinated inauthentic behavior" as shown in Figure 4. Facebook vouched to continue monitoring similar activities and declared that it would take action against those who commit further violations (Gleicher, 2019). Both Twitter and Facebook provided samples of the malicious content in their blogs and official statements.

Source: From Facebook (2019).

Figure 4. A sample from one of the pages taken down by Facebook that was classified as a coordinated and inauthentic behavior and was traced back to China.

CCP mouthpieces such as the *Global Times*, *People's Daily*, and the state-run *China Daily* attacked the actions of Facebook and Twitter, calling them "double standards." The Chinese-linked media called the crackdown a way of silencing the voices of Chinese netizens and suppressing public opinion and the freedom of speech. However, none of the Chinese state-owned media outfits stressed that Twitter and Facebook were both banned in China (Bloomberg, 2019).

The South China Sea Maritime Disputes

The South China Sea dispute is another interesting case study that perfectly demonstrates China's resolve in employing cyber coercion. Compared to Taiwan and Hong Kong, the South China Sea has a longstanding strategic and regional dimension as it involves not only the United States, but also majority of states situated in the Asia-Pacific who have an explicit or implicit interest in the issue.

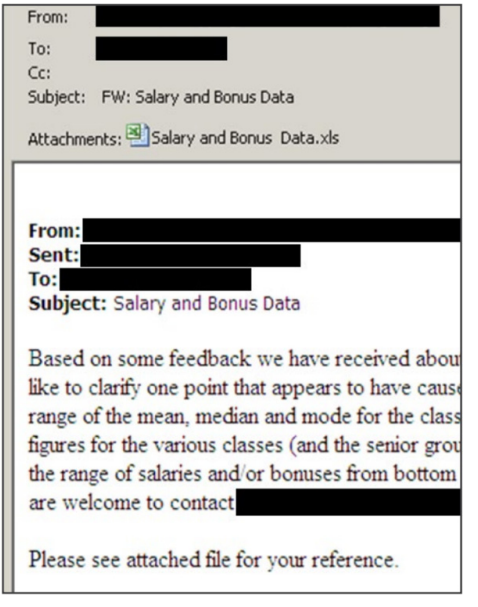
In recent years, growing scrutiny against China's "gray-zone strategy" in the contested waters has dominated mainstream media and policy discussions. However, very little attention has been devoted to China's deployment of cyber coercion to further its interests in the resource-rich waters. China's tools to impose its unilateral control in the South China Sea have evolved from its usual range of diplomatic, military, economic, and political arsenal. The use of cyber coercion completes the triad

of China's psychological warfare — overwhelming activities of Chinese maritime militia and the installation of missile systems to the artificial islands — designed to alter the equilibrium of the geopolitical status quo that is favorable to Beijing (Manantan, 2019b).

At the height of the standoff concerning the Scarborough Shoal and Spratly Islands in 2012, the Philippines and China were embroiled in a series of cyber conflicts (Passeri, 2012). Chinese hackers defaced official Philippine government websites and doxed information of government officials and media personalities. In retaliation, Filipino hacktivists took down Chinese-owned government websites and launched a worldwide cyber protest against Chinese aggression in the South China Sea and the West Philippine Sea (Passeri, 2012).

In 2015, FireEye published a report detailing the cyber espionage activities of Chinese-linked hackers in Southeast Asia to acquire information related to the growing tensions regarding the competing territorial claims. The attacks involved malware that targeted networks of critical industry sectors from energy, telecommunications, technology, transportation, to finance. However, the report highlighted the specific interest of Chinese-backed cyber operations in government and telecommunications systems and the energy sector. The findings revealed that Chinese-linked threat actors obtained sensitive information — "general military documents, internal communications, equipment maintenance reports and specifications, event related materials, documentation of organizational programs and initiatives" — for intelligence-gathering purposes (FireEye and Singtel, 2015). The APT group sent phishing emails and fake accounts that compromised intelligence agency email accounts. They targeted government and military officials who were responsible in "intelligence-sharing relationships" in relation to the maritime dispute (FireEye and Singtel, 2015). Meanwhile, three threat groups attempted to gain access to networks of oil companies which were conducting offshore oil exploration in the disputed waters. The PRC has a deep-seated interest in hydrocarbon reserves to guarantee a sustainable future energy supply that will sustain its economic growth (FireEye and Singtel, 2015, p. 8).

China's deployment of malware continued as the Philippines took the maritime dispute to a whole new level when it filed a formal complaint at the Permanent Court of Arbitration (PCA) at the Hague in 2015. The Philippines legally challenged China's expansive and aggressive behavior, specifically its *de facto* control of the territorial waters fueled by its sweeping nine-dash line claims. China has repeatedly dismissed the court case and refused to participate in the legal case. F-Secure Labs published a white paper in July 2016 exposing a malicious malware program called *NanHaiShu*. The recorded cyber espionage attacks which transpired from 2014 to 2016 have



Source: From F-Secure (2016).

Figure 5. Spear-phishing email sent to the law firm employees who represent nation-states in the arbitration case on the South China Sea disputes against China.

targeted the Department of Justice of the Philippines (DOJ), the Asia-Pacific Economic Cooperation (APEC) Summit organizing committee, and the major international law firm that represents nation-states in maritime disputes (Gontiga & Tan, 2016). The report also noted the significance of the targeted organizations who are at the epicenter of the South China Sea dispute which represents a high strategic value to Beijing (Gilbert, 2016).

Based on the detailed analysis illustrated in Figure 5, the report suggests that "the threat actor used spear-phishing email messages to deliver the malware to targets, with the text contents of the emails carefully crafted" (F-Secure, 2016). As a "Remote Access Trojan" or RAT, the attacker can download files and scripts that can be used to exfiltrate highly sensitive data from the targets. F-Secure contends that the *NanHaiShu* samples resembled codes and infrastructure that were tracked back to developers based in Mainland China, thus confirming that the intrusions were of Chinese origin.

The website of the PCA was also targeted by Chinese-backed spies at the height of the weeklong hearing at the Hague in July 2015 (Tweed, 2015). The website was infected by malware that exposes the landmark case of data theft (Healey & Piiparinen, 2015). Chinese cyber units can then access internal documents as well as identify

interested parties such as diplomats, lawyers, and journalists who are following the case.

After the Philippines won its arbitration case in July 2016 which invalidated China's exaggerated and baseless nine-dash claims, Chinese-linked cyber operations have increased as far as inflicting potential destruction to critical infrastructure. More than a week after the landmark victory for the Philippines, Vietnamese airlines suffered cyberattacks in two airports in Ho Chi Minh and Hanoi (H. Clark, 2016). As illustrated in Figure 6, the cyberattacks showed offensive messages on the flight information screens denouncing the Philippines and Vietnam while public announcement systems broadcasted a similar derogatory message (Kang, 2016). The Chinese-backed hacking group 1937CN initially claimed responsibility for the attack but later on retracted the statement. According to Vietnamese media, the group has been associated to other cyberattacks in Vietnam in the past.

Despite the perceived "pivoting" of Philippine President Rodrigo Duterte toward China that has been exemplified by the warming of political and economic ties, recent events in the South China Sea have prompted the Duterte government to reinvigorate its security reliance on the United States (Manantan, 2019b). The renewed strategic relations between Manila and Washington came as a surprise especially under Duterte, who has consistently adopted an anti-US stance. This has cemented the growing

Source: From Tatarski (2016).

Figure 6. Chinese-backed hacking group 1937CN displayed offensive messages on the information screens at Hanoi's Noi Bai International Airport and Tan Son Nhat International Airport in Ho Chi Minh City at the height of the South China Sea disputes.

dissatisfaction of the country with China's *de facto* control in the South China Sea which culminated in a maritime collision involving Chinese militia and Filipino fishermen within the Philippines Exclusive Economic Zone (EEZ) in June 2019 (Ranada, 2019). Upon Duterte's acceptance of US security assurances against future actions involving Chinese-linked maritime militia, an uptick of Chinese cyber operations infiltrating Philippine government websites was reported.

China also used its cyber capabilities to gather information related to the formulation of the first draft of the highly anticipated Code of Conduct (COC) in the South China Sea. As the overall coordinator of the COC, the Philippines has been facilitating dialogs and negotiations for the Single Draft Code of Conduct since in late November 2019. In a report published by enSilo, Chinese-linked APT10 deployed malicious software variants that targeted the Philippine government and private organizations in April 2019. The report also suggests that the malware, tactics, techniques, procedures, and codes were all uniquely identifiable to APT10 (Hunter, 2019). Within the same month, the Analytics Association of the Philippines identified Chinese-linked scripts that were inserted into the source codes of various government websites to collect information from target users (Panaligan, 2019).

Unpacking Chinese-Linked Cyber Coercion

The analysis of the three case studies confirms that *weishe* has become a cornerstone in Beijing's overall strategic arsenal, and two major trends have emerged. The first is the blurring distinction between what constitutes compellence or deterrence. China uses both simultaneously to impose both threats and the actual imposition of them. This allows China to convey a clear demand and/or provoke a definitive response from its target state or actor. To achieve coercion, China deploys sophisticated attacks — malware, phishing emails, and DDoS attack on targeted individuals and organizations — as well as low-level intrusions to exploit vulnerabilities or conduct cyber espionage. Notwithstanding the quality of cyberattacks, intelligence-gathering, surveillance, and network reconnaissance lie at the heart of PRC's cyber coercion. It allows Beijing to craft a pre-emptive strategy and/or adopt an offensive stance against its adversaries whether in war or peacetime.

Despite the overwhelming volume and the growing sophistication of the attacks, closer scrutiny reveals that cyber operations were persistent but of low level. Still, such an observation does not diminish the strategic leverage of the PRC's cyber coercion in creating the intelligence loss or gain dilemma, nor its resolve and commitment to further escalate the current threat. In fact, this perfectly captures the "psychological"

warfare dimension as the defining pillar in China's strategic doctrine stipulated in official documents and public statements. China remains circumspect not to elevate the threshold of its coercive activities in order to avoid any unintended consequences that might lead down the path of further escalation or inflict damage to critical infrastructures. Thus, to further cement its cyber coercion, Beijing leverages its vital assets that are available at its disposal rather than relying solely on its cyber capabilities. From its political, economic, and diplomatic enticements to its strong rhetoric issued through its official channels or state-owned media, Beijing is maximizing its pool of resources to deploy its coercive strategy of influencing the behavior of its targets without sparking conflict escalation.

The second trend points to the rising prominence of disinformation campaigns as a tool for cyber coercion by Chinese-sponsored hackers. There has been growing traction within the PRC and its proxies to capitalize on the ongoing political, economic, and social discontent to undermine the overall stability of Taiwan and Hong Kong. Social media platforms and online messaging applications have become critical hotbeds for the PRC and its proxies to spread fake news, incite conspiracies, and prosecute political actions. Hence, where compellence or deterrence begins and ends is not clear cut, and to a certain degree both are even mutually reinforcing and allow the PRC to shape its external environment to achieve its goals.

Interestingly, Chinese-linked hackers are not only launching coercive attacks against nation-states or governments but also targeting or threatening the general public via social media applications or through public communication systems. This applies to the domestic population of Taiwan, Hong Kong, the Philippines, and Vietnam. The PRC's interest in exploiting social media to undermine democratic values and institutions and to instigate social unrest illustrates that it does not discriminate between governments and the general public. This further confirms the previous observation of how disinformation campaigns have become an emerging trend in the PRC's broader coercive strategy.

The analysis of the three case studies also builds a strong argument for the role of contextual and operational dimensions in detecting and responding to China's imminent cyber coercion. Overall, the geopolitical climate is a contextual indicator which lays the foundation for China to unleash its cyber army. The PRC's interest both in unseating the ruling DPP party in Taiwan in the 2020 election and diminishing Hong Kong's autonomy lays fertile ground for China to conduct cyber espionage or information warfare. At the same time, the intensifying territorial claims in the South China Sea especially in the lead up to the filing of the arbitration case and the subsequent

release of the landmark ruling prompted Chinese-backed hackers to engage in intelligence-gathering against government, military institutions, and private companies.

The growing historical records of Chinese cyberattacks confirmed by various private cybersecurity firms, government agencies, and non-governmental institutions provide a strong technical catalogue in identifying exploits, tactics, techniques, and procedures that are unique to Chinese-linked hackers. The trends and patterns that reflect the emergence and re-emergence of Chinese-linked cyber army groups with unique TTPs combined with IP addresses that can be traced back to China provide a viable solution in mitigating the attribution challenge. Considering the contextual and operational factors thus provides the general parameters in the emergence of PRC-backed cyber coercion.

Both contextual and operational dimensions were essential in understanding how the threatened state or non-state actors countered PRC-linked cyber coercion. Detecting the sudden surge in malicious cyber activity at the height of political contestation was a trigger point among states to directly respond to Chinese-linked cyber coercion. Taiwan, Vietnam, and the Philippines have diplomatically called out China's cyberattacks, which the latter has consistently denied. Taiwan and the Philippines have sought to invoke their security partnerships with the United States. Taiwan and the US have also conducted a joint-cyberwar drill in response to the alarming interference of Chinese-linked cyber operations ("US and Taiwan," 2019). Furthermore, in response to China's systems intrusions and for the purposes of sending a "warning" to China that it has been detected, Taiwan has deliberately made such hostile activities public. To counter the proliferation of red media infiltration, the Taiwanese government is being urged to pass laws that will require foreign agents to register with the government (Fang, 2019).

In the era of hyper-connectivity where cyber operations are conducted instantaneously, non-state actors have also taken proactive roles against suspected PRC-linked proxies without relying too much on governments or nation-states. As demonstrated by the actions undertaken by Facebook, Twitter, and Telegram, a definitive response was launched after a threshold was reached. This is characterized by a highly coordinated and large-scale movement emanating from fake accounts and/or known threat actors set at the backdrop of the intensifying Hong Kong protests.

Facebook and Twitter's self-regulation policies for inauthentic and coordinated malicious behavior can be considered as agile responses to Chinese-backed operations. They have suspended or banned fake accounts under their own jurisdictions. This exercise of self-regulation among social media giants has become a critical tool in countering the spread of fake news and disinformation campaigns against a group or

individual protesters which ultimately undermines the PRC's coercive actions. In the midst of China's massive cyberattack, Telegram was able to recover after the "state-sponsored" DDoS attack while ensuring that it has protected the data of its users (Barbaschow, 2019). Following the attack, Telegram also made a fundamental change to its system by safeguarding the identities of protesters participating in group chats. This was an unprecedented step undertaken by the messaging app to "counter mass-importing attempts" and add another layer of privacy (Doffman, 2019).

Conclusion

As shown by the growing interconnectedness and vulnerability of state and non-state actors as potential targets of Chinese-linked proxies, it is imperative for both to start exploring greater collaboration in countering cyber coercion. The reports published by cybersecurity firms highlight the opportunity afforded by threat-information-sharing initiatives to better understand the emergence and/or likelihood of cyber coercion-related attacks.

Despite their noble intent, however, threat-information-sharing mechanisms have remained a contentious subject between the private and public sectors contingent on the extent of collaboration and available resources between parties. It also raises serious questions on the varying cybersecurity capabilities and investment of the private and public sectors. Yet as Chinese cyber coercion in the three case studies has demonstrated, every actor is a potential target. This creates a greater incentive for all parties to cooperate provided that the designation of specific deliverables and the identification of clear-cut expectations from both parties are neatly arranged.

The paper's overall analysis brings key lessons to the fore that could be pursued within the public–private partnership that include sharing the best practices and adopting self-regulatory frameworks as demonstrated by Facebook, Twitter, and Telegram. Recognizing the increasing importance of cybersecurity as a national security priority, governments have also started to produce their respective National Cyber Security Strategies, especially in the case of Southeast Asian countries. At the same time, Taiwan has started to explore the ratification of laws that could penalize foreign interference. To achieve a real impact, however, the vision and strategies set forth in such documents must be matched with adequate resources, reflect the changing threat landscape, and value equitable partnership among all key stakeholders.

As China pursues its self-declared ambition of national rejuvenation as shown in the triumvirate of Taiwan, Hong Kong, and the South China Sea, the deployment of

cyber coercion — in sync with diplomatic, economic, and political tools — will remain a fundamental hallmark of its hybrid warfare. On top of its ongoing consolidation of defense and security capabilities to complement its growing political and economic influence, China will continue to invest in this kind of asymmetrical capacity. The trends that have emerged from the analysis in this paper expose the fluidity of compellence and deterrence from the vantage point of the PRC. It is a testament to the level of sophistication that the PRC currently possesses to coerce using varying degrees and types of cyberattacks.

As Chinese-linked cyber operations continue to expand in terms of scope and depth, the paper's emphasis on both contextual and operational dimensions is a significant contribution that helps non-technical experts and practitioners to better understand coercion in the cyber domain. It is an attempt to explicate practical insights on how key stakeholders from the public and private sectors can collaborate to counter cyber coercion in the evolving threat landscape.

Acknowledgments

This publication was funded by the Taiwan Research Fellowship by the Ministry of Foreign Affairs, Republic of China (Taiwan).

References

Barbaschow, A. (2019). Telegram says "whooper" DDoS attack launched mostly from China. *ZDNet.* Retrieved from https://www.zdnet.com/article/telegram-says-whopper-ddos-attack-launched-mostly-from-china/.

Bloomberg (2015, December 21). Chinese hackers increase attacks on Taiwan opposition before January's presidential election: US security firm. *South China Morning Post.* Retrieved from https://www.scmp.com/news/china/diplomacy-defence/article/1893663/chinese-hackers-increase-attacks-taiwan-opposition.

Bloomberg (2019, August 20). Chinese paper attacks Twitter and Facebook for shutting accounts. *Bloomberg.* Retrieved from https://www.bloomberg.com/news/articles/2019-08-20/china-paper-attacks-twitter-and-facebook-for-shutting-accounts.

Chase, M., & Chan, A. (2016, June 28). *China's evolving approach to integrated strategic deterrence.* Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1366/RAND_RR1366.pdf.

Cheng, D. (2011). Chinese views on deterrence. *Joint Force Quarterly*, *60*, 92–94.

Clark, H. (2016, August 6). The alleged Chinese hacking at Vietnam's airports shows that the South China Sea battle isn't just in the water. *Huffpost.* Retrieved from https://www.huffpost.com/entry/china-hack-vietnam-south-china-sea_b_11357330.

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it.* New York, NY: HarperCollins.

Costelo, J., & McReynolds, J. (2018). *China's strategic support force: A force for a new era.* Washington, DC: National Defense University Press.

Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid war: High-tech, information and cyber conflicts. *Connections: The Quarterly Journal*, *16*(2), 5–24. Retrieved from https://connections-qj.org/article/hybrid-war-high-tech-information-and-cyber-conflicts.

Doffman, Z. (2019, August 31). Shock Telegram change protects Hong Kong protesters from China — But 200M users affected. *Forbes.* Retrieved from https://www.forbes.com/sites/zakdoffman/2019/08/31/new-telegram-shock-encrypted-app-changes-for-200m-users-to-protect-hk-protesters/#7b749f158760.

Facebook (2019, August 19). Image-5. Retrieved from https://about.fb.com/wp-content/uploads/2019/08/image-5.png.

Fang, F. (2019, July 29). Taiwan professors call on government-run companies, agencies to stop subscribing to pro-Beijing media. *The Epoch Times.* Retrieved from https://www.theepochtimes.com/taiwan-professors-call-on-government-run-companies-and-agencies-to-stop-subscribing-to-pro-beijing-media_3020704.html.

FireEye (2019). *Double dragon: APT41, a dual espionage and cyber crime operation.* Retrieved from https://content.fireeye.com/apt-41/rpt-apt41/.

FireEye and Singtel (2015, March). *Southeast Asia: An evolving cyber threat landscape.* Retrieved from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf.

Fleming, D. R., & Rowe, N. C. (2015). Cyber coercion: Cyber operations short of cyberwar. In *Proceedings of 10th International Conference on Cyber Warfare and Security*, Skukuza, South Africa. Retrieved from https://faculty.nps.edu/ncrowe/oldstudents/flemming_iccws15.htm.

F-Secure (2016). *NanHaiShu: RATing the South China Sea.* Retrieved from https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf.

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*, *38*(2), 41–73. doi: 10.1162/ISEC_a_00136.

Gilbert, D. (2016, August 4). Chinese hackers thought to target Philippines over South China Sea dispute. *Vice.* Retrieved from https://www.vice.com/en_us/article/vv7zy3/chinese-hackers-thought-to-target-philippines-over-south-china-sea-dispute.

Gleicher, N. (2019, August 19). Removing coordinated inauthentic behavior from China. Retrieved from Facebook website: https://about.fb.com/news/2019/08/removing-cib-china/.

Gold, M. (2013, July 19). Taiwan a "testing ground" for Chinese cyber army. *Reuters.* Retrieved from https://www.reuters.com/article/net-us-taiwan-cyber-idUSBRE96H1-C120130719#:~:text=TAIPEI%20(Reuters)%20%2D%20Taiwan%20is,ties%20with%20the%20United%20States.

Gomez, M. (2018). When less is more: Cognition and the outcome of cyber coercion. *Cyber, Intelligence, and Security*, *2*(1), 3–19. Retrieved from https://www.inss.org.il/publication/when-less-is-more-cognition-and-the-outcome-of-cyber-coercion/.

Gontiga, J. C., & Tan, L. (2016, August 5). Suspected Chinese malware used to spy on PH gov't-security firm. *CNN Philippines.* Retrieved from http://nine.cnnphilippines.com/news/2016/08/05/South-China-Sea-RAT-cyber-attack-Philippines.html.

Groll, E. (2017, November 30). Feds quietly reveal Chinese state-backed hacking operations. *Foreign Policy.* Retrieved from https://foreignpolicy.com/2017/11/30/feds-quietly-reveal-chinese-state-backed-hacking-operation/.

Healey, J., & Piiparinen, A. (2015, October 27). Did China just hack the international court adjudicating its South China Sea territorial claims? *The Diplomat.* Retrieved from https://thediplomat.com/2015/10/did-china-just-hack-the-international-court-adjudicating-its-south-china-sea-territorial-claims/.

Hodgson, Q., Ma, L., Marcinek, K., & Schwindt, K. (2019). *Fighting shadows in the dark understanding and countering coercion in cyberspace.* Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2961/RAND_RR2961.pdf.

Huang, P. (2019, June 26). Chinese cyber-operatives boosted Taiwan's insurgent candidate. *Foreign Policy.* Retrieved from https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/.

Hunter, B. (2019, May 24). *Uncovering new activity by APT10.* Retrieved from enSilo Intelligence Team website: https://blog.ensilo.com/uncovering-new-activity-by-apt10.

Ihara, K. (2019, September 12). In Beijing rebuke, Taiwan signals closer defense ties with US and Japan. *Nikkei Asian Review.* Retrieved from https://asia.nikkei.com/Politics/International-relations/In-Beijing-rebuke-Taiwan-signals-closer-defense-ties-with-US-and-Japan.

Jensen, B. (2019, June 20). *What a U.S. operation in Russia shows about the limits of coercion in cyber space* [Commentary]. Retrieved from War on the Rocks Media, LLC website: https://warontherocks.com/2019/06/what-a-u-s-operation-in-russia-shows-about-the-limits-of-coercion-in-cyber-space/.

Kang, H. (2016, July 29). Flight information screens in two Vietnam airports hacked. *Reuters in Hanoi.* Retrieved from The Guardian website: https://www.theguardian.com/world/2016/jul/29/flight-information-screens-in-two-vietnam-airports-hacked.

Kolton, M. (2017). Interpreting China's pursuit of cyber sovereignty and its views on cyber deterrence. *The Cyber Defense Review*, *2*(1), 119–154. Retrieved from www.jstor.org/stable/26267405.

Kumar, M. (2019, June 13). Telegram suffers "powerful DDoS attack" from China during Hong Kong protests. *The Hacker News.* Retrieved from https://thehackernews.com/2019/06/telegram-ddos-attack.html.

Kurlantzick, J. (2019, November 7). *How China is interfering in Taiwan's election.* Retrieved from the Council on Foreign Relations website: https://www.cfr.org/in-brief/how-china-interfering-taiwans-election.

Lee, Y. (2019, August 10). Taiwan urges citizens to stay on alert for China-backed media infiltration. *Reuters.* Retrieved from https://www.reuters.com/article/taiwan-china-media-reaction/taiwan-urges-citizens-to-stay-on-alert-for-china-backed-media-infiltration-idUSL4N256074.

Lewis, J. (2011). Cyberwar thresholds and effects. *IEEE Security & Privacy*, *9*(5), 23–29. doi: 10.1109/MSP.2011.25.

Manantan, M. (2019a, March 4). How Taiwan stands up to China through soft power [Commentary]. *The Philippine Star.* Retrieved from https://www.philstar.com/other-sections/news-feature/2019/03/04/1898588/commentary-how-taiwan-stands-china-through-soft-power#HzH0vzCl0YrzV1Sg.99.

Manantan, M. (2019b, July 4). Cyber dimension of the South China Sea clashes. *The Diplomat.* Retrieved from http://thediplomat.com/2019/08/the-cyber-dimension-of-the-south-china-sea-clashes/?allpages=yes&print=yes.

Mayberry, K. (2019, June 11). Hong Kong's controversial extradition bill explained. *Aljazeera.* Retrieved from https://www.aljazeera.com/news/2019/06/explainer-hong-kong-controversial-extradition-bill-190610101120416.html.

McWhorter, D. (2013). Mandiant exposes APT1-One of China's cyber espionage units & releases 3,000 indicators. Retrieved from FireEye website: https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html.

Mozur, P., & Stevenson, A. (2019, June 13). Chinese cyberattack hits Telegram, app used by Hong Kong protesters. *The New York Times.* Retrieved from https://www.nytimes.com/2019/06/13/world/asia/hong-kong-telegram-protests.html.

Neuman, C., & Poznansky, M. (2016, June 28). *Swaggering in cyberspace: Busting the conventional wisdom on cyber coercion* [Commentary]. Retrieved from War on the Rocks Media, LLC: https://warontherocks.com/2016/06/swaggering-in-cyberspace-busting-the-conventional-wisdom-on-cyber-coercion/.

Office of Public Affairs. (2018, December 20). *Two Chinese hackers associated with the Ministry of State Security charged with global computer intrusion campaigns targeting intellectual property and confidential business information.* Retrieved from the United States Department of Justice website: https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

O'Flaherty, K. (2019, June 13). Telegram hack blamed on China coincides with Hong Kong protests. *Forbes.* Retrieved from https://www.forbes.com/sites/kateoflahertyuk/2019/06/13/telegram-hack-blamed-on-china-as-protests-take-place-in-hong-kong/#2fe0fd581c3c.

Osborne, C. (2016, September 13). Chinese hackers take down Vietnam airport systems. *ZDNet.* Retrieved from https://www.zdnet.com/article/chinese-hackers-take-down-vietnam-airport-systems/.

Panaligan, M. (2019, April 1). Analytics consultant discovers "strange" script with links to China on gov't websites. *GMA News Online.* Retrieved from https://www.gmanetwork.com/news/scitech/technology/689936/analytics-consultant-discovers-strange-script-with-links-to-china-on-gov-t-websites/story/.

Passeri, P. (2012, May 1). *Philippines and China, on the edge of a new cyber conflict?* Retrieved from Hackmageddon website: https://www.hackmageddon.com/2012/05/01/philippines-and-china-on-the-edge-of-a-new-cyber-conflict/.

Ranada, P. (2019, July 6). Final PCG-Marina report: Chinese shop failed to prevent sea collision. *Rappler.* Retrieved from https://www.rappler.com/nation/234700-chinese-ship-failed-prevent-sea-collision-final-coast-guard-marina-report-june-2019.

Schelling, T. (1966). *Arms and influence.* New Haven, CT: Yale University Press.

Segal, A. (2018, December 6). *A new old threat.* Retrieved from the Council on Foreign Relations website: https://www.cfr.org/report/threat-chinese-espionage.

Shanapinda, S. (2019, June 14). How a cyber-attack hampered Hong Kong protesters. *The Conversation.* Retrieved from https://theconversation.com/how-a-cyber-attack-hampered-hong-kong-protesters-118770.

Sharp, T. (2017). Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies*, *40*(7), 898–926. doi: 10.1080/01402390.2017.1307741.

Shieber, J. (2019, June 13). Telegram faces DDoS attack in China… again. *TechCrunch.* Retrieved from https://techcrunch.com/2019/06/12/telegram-faces-ddos-attack-in-china-again/.

Shou, X. (2013). *The science of military strategy.* Beijing, China: Military Science Press.

Spencer, D. (2018, July 13). Why the risk of Chinese cyberattacks could affect everyone in Taiwan. *Taiwan News.* Retrieved from https://www.taiwannews.com.tw/en/news/3481423.

Spencer, D. (2019, February 24). Taiwan needs to take cybersecurity seriously at the highest level. *Taiwan News.* Retrieved from https://www.taiwannews.com.tw/en/news/3644195.

Tatarski, M. (2016, August 9). China 1937CN Team infiltrate Vietnam airlines, airports. *AEC News Today.* Retrieved from https://aecnewstoday.com/2016/hack-vietnam-airports-highlights-weaknesses/.

Timeline: Key dates in Hong Kong's anti-government protests. (2019, November 11). *Reuters.* Retrieved from https://www.reuters.com/article/us-hongkong-protests-timeline/timeline-key-dates-in-hong-kongs-anti-government-protests-idUSKBN1XL0N3.

Torde, G. (2019, June 6). Why Hong Kong's extradition law changes are fueling fears. *Reuters.* Retrieved from https://www.reuters.com/article/us-hongkong-politics-extradition/why-hong-kongs-extradition-law-changes-are-fuelling-fears-idUSKCN1T70OA.

Tweed, D. (2015, October 16). China's cyber spikes take to high seas as hack attacks spike. *Bloomberg.* Retrieved from https://www.bloomberg.com/news/articles/2015-10-15/chinese-cyber-spies-fish-for-enemies-in-south-china-sea-dispute.

Twitter, Inc. (2019, August 19). *Updating our advertising policies on state media.* Retrieved from https://blog.twitter.com/en_us/topics/company/2019/advertising_policies_on_state_media.html.

Twitter Safety. (2019, August 19). *Information operations directed at Hong Kong.* Retrieved from https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html.

Uren, T., Thomas, E., & Wallis, J. (2019, September 12). *Tweeting through the Great Firewall.* Retrieved from Australian Strategic Policy Institute website: https://www.aspi.org.au/report/tweeting-through-great-firewall.

US and Taiwan hold first joint cyber-war exercise. (2019, November 4). *BBC.* Retrieved from https://www.bbc.com/news/technology-50289974.

US approves possible $2.2bn arms sale to Taiwan. (2019, July 9). *Aljazeera.* Retrieved from https://www.aljazeera.com/news/2019/07/approves-22bn-arms-sale-taiwan-190708233858400.html.

Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion.* New York, NY: Oxford University Press.

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research*, *51*(3), 347–360. doi:10.1177/0022343313518940.

Wang, Z. (2007). *Information confrontation theory.* Beijing, China: Military Science Press.

Waxman, M. (2013). Self-defensive force against cyber attacks: Legal, strategic and political dimensions. *International Law Studies*, *89*, 109–122.

Winters, R. (2015, December 21). *The EPS awakens — Part 2.* Retrieved from the FireEye website: https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html.

Wood, D., McMinn, S., & Feng, E. (2019, September 17). China used Twitter to disrupt Hong Kong protests, but efforts began years earlier. *NPR.* Retrieved from https://www.npr.org/2019/09/17/758146019/china-used-twitter-to-disrupt-hong-kong-protests-but-efforts-began-years-earlier.

Yu, J. (2018, June 15). Chinese cyberattacks on Taiwan government becoming harder to detect: Source. *Reuters.* Retrieved from https://www.reuters.com/article/us-taiwan-china-

cybersecurity/chinese-cyber-attacks-on-taiwan-government-becoming-harder-to-detect-source-idUSKBN1JB17L.

Zheng, S. (2019, September 17). Re-elect President Tsai Ing-wen in 2020 and Taiwan will lose all its allies, Beijing warns. *South China Morning Post.* Retrieved from https://www.scmp.com/news/china/diplomacy/article/3027673/re-elect-president-tsai-ing-wen-2020-and-taiwan-will-lose-all.