Issues & Studies

A Social Science Quarterly on China, Taiwan, and East Asian Affairs

Vol. 56 • No. 3 • September 2020

Editor-in-Chief
Chien-wen Kou
National Chengchi University

INSTITUTE OF INTERNATIONAL RELATIONS
NATIONAL CHENGCHI UNIVERSITY, TAIPEI, TAIWAN (ROC)

World Scientific

Issues & Studies

A Social Science Quarterly on China, Taiwan, and East Asian Affairs

Issues & Studies

A Social Science Quarterly on China, Taiwan, and East Asian Affairs

Vol. 56 • No. 3 • September 2020

Editor-in-Chief
Chien-wen Kou
National Chengchi University

INSTITUTE OF INTERNATIONAL RELATIONS
NATIONAL CHENGCHI UNIVERSITY, TAIPEI, TAIWAN (ROC)

World Scientific

Issues & Studies (IS)

Subscriptions, changes of address, single-copy orders should be addressed to Journal Department, World Scientific Publishing Co. Pte. Ltd., 5 Toh Tuck Link, Singapore 596224, or World Scientific Publishing Co, Inc, 27 Warren Street, Suite 401-402, Hackensack, NJ 07601, USA or 57 Shelton Street, Covent Garden, London WC2H 9HE, UK.

Articles and books for review should be sent to *Issues & Studies*, Institute of International Relations, National Chengchi University, No. 64, Wanshou Road, Wenshan District 116, Taipei City, Taiwan (ROC).

ROC Government Information Office, Certificate of Publishing Business Registration, No. 0999. Taipei Post Office, Chunghwa Post, Certificate of Journal Registration, No. 1029.

Typeset by Stallion Press
Email: enquiries@stallionpress.com

Issues & Studies

A Social Science Quarterly on China, Taiwan, and East Asian Affairs

Vol. 56, No. 3 **September 2020**

CONTENTS

Special Issue: Multidimensional Security Issues in Asia
Guest Editor: Chyungly Lee

Issues & Studies: A Social Science Quarterly on China, Taiwan,
and East Asian Affairs
Vol. 56, No. 3 (September 2020) 2002003 (5 pages)

DOI: 10.1142/S1013251120020038

Introduction to the Special Issue — Multidimensional Security Issues in Asia

Chyungly Lee

* * *

Multidimensional security issues in Asia, ranging from geostrategic rivalries and armed confrontations to transnational/transboundary and human security concerns, have been vigorously studied and well documented. This Special Issue is by no means to provide an inclusive digest. Instead, selection of the articles is based on contrastive research interests with hopes to bridge topics that are related but not often simultaneously presented and to help outlining a more comprehensive picture of Asian security.

The first set includes two longstanding but parallel Asian security agendas: the most striking element of Asian security architecture, the US-led hub-and-spoke alliance system, and a less attended but essential internal security subject, Papua separatism in Indonesia. The second set, in contrast, discusses the relatively new and sophisticated security issue of China's cyber threats. The strategic thinking of China's cyber coercion will be discussed first, followed by the critiques on regional responses based on the cyber deterrence theories.

Often known as the hub-and-spoke alliance system, the network of bilateral alliances created by the United States after World War II, continues to be an important topic in Asian security. In addition to inquiries into each bilateral story, what has puzzled many at the regional level is why the United States as the hub of this system did not create a NATO-like multilateral architecture in Asia. The powerplay theory presented by Victor Cha a decade ago has made an attempt to solve this puzzle. It suggests that through constructing asymmetric alliances, the United States intends to exert maximum control over the actions of its smaller allies and constrain anti-communist allies in the region from engaging in aggressive behavior against

Chyungly Lee (李瓊莉) is a Distinguished Research Fellow of the Institute of International Relations at National Chengchi University, Taiwan. Her research interests include Asia-Pacific comprehensive security, Asia-Pacific multilateralism, and conflict prevention in East Asia. She can be reached at <cllee@nccu.edu.tw>.

adversaries that could entrap the US in an unwanted larger war (Cha, 2009/2010). The first article of this Special Issue extends the discourse on choices between bilateralism and multilateralism in the current context and suggests that US preference remains as the main determinant for the prospect of security cooperation in Asia.

Ping-Kuei Chen applies the theories of alliance management and organization politics to analyze how the United States has enjoyed bargaining advantages over burden-sharing and policy coordination in dealing with its smaller allies bilaterally in recent years. Even as the bilateral and minilateral inter-alliance cooperation and partnership have significantly increased in response to China's recent assertiveness, **Chen** argues that the emergence of a sophisticated multilateral security mechanism is unlikely and that a NATO-like defense pact in Asia remains even less so. As long as the US continues to be able to push the defense policies of its allies to accommodate its interests, it is likely to prefer the hub-and-spoke alliance system over multilateral arrangements. Moreover, the escalation of the strategic tension between the US and China in the Trump administration has made the US allies less autonomous in security policymaking. Consequently, the hub-and-spoke alliance system could continue to favor the US security interests.

In contrast to geopolitics and geostrategic calculations which dominate the security perceptions of regional powers, internal security and nation-building seem to be more critical to countries in Southeast Asia. Like many countries in the region, Indonesia is a multi-ethnic, multi-religious, and multi-linguistic country with wide economic disparity. Terrorism, separation, societal incoherence, and transnational crimes are often considered major internal security threats to Indonesia (de Haan, 2019). The sources of these threats, however, mostly originate in economic, ethnic, and religious tensions. Domestic security thus heavily relies on the regime's performance in delivering continuous economic growth and sustaining societal coherence. Accordingly, Papua in Indonesia's security calculations rests on its geographical, cultural, and ethnic periphery. Being at the margins has conversely given Papua a defining role in Indonesia's nation-state building and territorial integrity. Nevertheless, this so-called security approach adopted in the past seemed to have counterproductively consolidated a separate Papuan identity and strengthened a desire for Papuan independence (Chauvel & Bhakti, 2004). Encouraged by the success of international intervention in East Timor's independence, Papua separatists intensified their use of the Pacific Islands Forum (PIF) and other international forums as venues to gain international support. In response, the Indonesian government granted a special autonomy status to Papua in 2001 and initiated the Southwest Pacific Dialogue group in 2002 to search for a peaceful resolution.

In the second article, **Baiq Wardhani and Vinsenio Dugis** examine foreign aid, another proactive peaceful approach taken by the Indonesian government in recent years. In addition to working with Papuans, the Indonesian government has used development assistance to the South Pacific region as a diplomatic instrument to shape a favorable international environment, hoping to decrease external support for Papuan separatism. The authors argue that Indonesia is portraying a new image of a recipient-turned-donor country based on a combination of its achievements in the successful management of foreign debt, its "prosper-thy-neighbor" policy, and its regional power strategy. Together with development partners, Indonesia has committed to the strengthening of regional processes and institutions and the facilitation of South–South Cooperation. The authors agree that this strategy of "winning the hearts of the people" has shown positive results and that PIF's support for Papuan separatism has not recently intensified.

As for the emerging security agenda, the two irreversible trends of technological advancement in ICT industries and the innovative evolution of social media have prompted cyberspace to be one of the most dynamic domains in the shaping of Asian security environment. Cyber threats to national and regional security can often be seen in two types: attacks against the physical layer of cyberspace and cyber-enabled information warfare. The former refers to more direct hacking into ICT or information-controlled critical infrastructures, while the latter is indeed a psychological battle of influencing. Both have been employed as tactics in realizing Chinese traditional strategic thinking that aims at winning a battle without fighting a physical war. More complicatedly, China's strategic calculations in cyberspace are often in line with the concept of omnipresent struggle which blurs the distinction between wartime and peacetime. Cyber operations thus are not limited to time or space. For regional countries constantly under a cyber threat from China, more innovative response strategies might be needed.

In the third article, **Mark Bryan Manantan** applies the concept of coercion to analyze how China uses cyber operations, launched by both military and civilian entities or proxies, to advance its three core national interests: Taiwan, Hong Kong, and the South China Sea. **Manantan** takes the Chinese term "weishe" to be roughly equivalent to Thomas Schelling's notion of coercion that entails both deterrence and compellence. The study of those three cases confirms that "weishe" remains a cornerstone of Beijing's overall strategic arsenal. The strategy of cyber coercion, integrated with other forms of hybrid warfare and disinformation campaigns, allows China simultaneously to impose threats and the actual imposition of them to convey a clear demand and/or provoke a definitive response from its target state or actor. By adopting

such an approach that blurs the distinction between deterrence and compellence, China effectively uses its cyber forces in information-based battles.

Taiwan and Japan are the two most vulnerable countries to China's cyber threats. Both have recently pronounced their countering strategies which are targeted at deterring China's state-sponsored cyberattacks. In the fourth article, **Hon-min Yau** revisits the applicability of nuclear deterrence theory in cyberspace and suggests an alternative concept of cyber cooperation to better cope with the limits of cyber deterrence. Although **Yau** highlights the need for well-coordinated responses from like-minded countries to defend time-sensitive cyber threats, he cannot deny the possible cheating problem in international collaboration. Nevertheless, the author argues that in the cyber domain, a defensive posture can hardly be misinterpreted as an offensive one because the increase of cybersecurity cannot possibly make others less secure directly. The differentiation between offense and defense postures, according to Robert Jervis's thesis on cooperation under the security dilemma, makes cyber cooperation possible.

It goes without saying that the topics of the four articles selected in this Special Issue are just the tip of the iceberg in Asian security studies. Nevertheless, at least three trends are suggested here to be worthy of scholarly attention.

First, the Asian security environment continues to evolve against the dynamics of US–China geostrategic competition at both global and regional levels. For relatively small/weak regional countries, searching for strategic autonomy to maximize national interests, including adopting a hedging strategy, has been and will continue to be a prevailing but structurally constrained objective in security calculations.

Second, the alleged domestic security issues with direct confrontations among autonomous entities indeed have strong international and regional politico-economic implications. All the parties involved have tried and will continue to employ external resources to win the battles. The argumentation line between domestic and international security issues has gradually blurred.

Third, effective responses to non-conventional sources of security threats, including climate change, economic disparities, pandemic issues, mass migration, or cyberspace, often require substantial multilateral inter-state collaboration. Unfortunately, the management of collective responses can hardly be free of geopolitics. The recent COVID-19 crisis exemplifies how a public health issue has evolved from health security concerns into world pandemic politics. Therefore, transnational/transboundary sources of security threats cannot only be diagnosed within the so-called nontraditional security paradigm.

References

Cha, V. (2009/2010). Origins of the U.S. alliance system in Asia. *International Security*, *34*(3), 158–196.

Chauvel, R., & Bhakti, I. (2004). *The Papua conflict: Jakarta's perceptions and policies*. Washington, DC: The East-West Center.

de Haan, J. (2019, February 21). *Indonesia: Threats and challenges to domestic security.* (Strategic Analysis Paper). Retrieved from http://www.futuredirections.org.au/publication/indonesia-threats-and-challenges-to-domestic-security/.

Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs
Vol. 56, No. 3 (September 2020) 2040012 (34 pages)

DOI: 10.1142/S1013251120400123

The Prospects of the US Alliance System in Asia: Managing from the Hub

Ping-Kuei Chen

This paper examines the implications of the United States' "hub-and-spoke" alliance system in Asia. It argues that the US enjoys a bargaining advantage in the current bilateral security relations with its Asian allies. In contrast to a multilateral alliance, the US can better prevent free riders and joint resistance in its bilateral relations. It can effectively restrain the behavior of its allies and compel them to accommodate American interests. The hub-and-spoke system helps the US consolidate its policy influence over the Asian allies, supervise inter-alliance cooperation, and increase defense cooperation between allies and non-allies. This paper uses episodes of defense cooperation between the US, Japan, South Korea, Australia, and India to illustrate the American alliance management techniques since 2016. During this time, the US allies have increasingly participated in regional security affairs due to US demands and guidance rather than autonomous decisions. Facing strong US pressure, allies have found it hard to challenge the US under the hub-and-spoke system despite common grievances. This leads to two implications for the future: First, the US allies may have less autonomy in their foreign policies, restraining their ability to pursue neutral positions and policies in regional affairs such as the South China Sea dispute. Second, the US may discourage or even undermine the emergence of multilateral security institutions in Asia. The US is likely to maintain the "hub-and-spoke" system to safeguard its strategic interests in the Indo-Pacific.

Keywords: Hub-and-spoke; US–Japan alliance; US–Australia alliance; US–ROK alliance; the Quad.

* * *

論 Since the end of World War II, American alliance policies in East Asia have been characterized by a "hub-and-spoke" system that consists of bilateral alliances organized by the United States, a system which was originally

Ping-Kuei Chen (陳秉逵) is an Associate Professor at the Department of Diplomacy, College of International Affairs, National Chengchi University, Taiwan. His research interests include conflict studies, security institutions, alliance cohesion, East Asian affairs, Cross-Strait relations, and global governance. He can be reached at <pkchen@nccu.edu.tw>.

designed to serve its strategic interests. This system also coped with historic conflicts between Japan, South Korea, and Taiwan during the early days of the Cold War (Cha, 2016; Hemmer & Katzenstein, 2002). Over time, Japan, South Korea, and Australia have become the key allies of the United States under this "hub-and-spoke" system and the main vehicles for the projection of its power. They provide forward bases for US armed forces, share intelligence and weapon systems, offer logistics should the US use force in the Pacific, and even send combat forces to join the US in armed conflicts. Each alliance serves a different purpose and targets a different security threat. Since the end of the Cold War, these allies have each remained loyal to their respective US alliances while building and consolidating military cooperation with the US.

Recently, the US has faced heightened security challenges in East Asia. The rise of China's military strength and its foreign policy choices have been of utmost concern. As China has fortified the occupied South China Sea land features to defend its territorial and maritime claims, the US and other regional actors have been worried about the country's intentions. Across the Taiwan Strait, China has intensified its diplomatic and military pressure since the election of President Tsai Ing-wen. The territorial dispute between Japan and China over the Senkaku/Diaoyu Islands has cooled down over the last few years, but China has continued to employ non-militarized measures to challenge Japan's ownership. Similarly, the North Korea regime under Kim Jong-un has remained a genuine security threat to South Korea, Japan, and American military personnel stationed in Far East. To cope with these security challenges, the US began to refocus on East Asia during the Obama administration. Obama's "pivot to Asia" or "rebalancing" increased the American military presence and economic engagement in the region. The Trump administration continued this policy posture and later declared a "Free and Open Indo-Pacific Strategy (FOIPS)." Under these mandates, both administrations increased the US military presence in East Asia and strengthened defense cooperation with allies.

In addition to diverting military assets to the Indo-Pacific, the US has adjusted its alliance policies and requested that its Asian allies take more responsibility in regional security affairs. These allies were asked to increase defense spending and to join overseas operations. Japan, in particular, has adopted many new initiatives. The Japan Maritime Self-Defense Force (JMSDF) participated in joint exercises with South Korea, India, the Philippines, and Australia. Japanese vessels joined naval drills with the United States Navy and other allies in the South China Sea. South Korea agreed to deploy the Terminal High Altitude Area Defense (THAAD) system amidst a nuclear threat from Pyongyang. South Korea, Japan, and the US held multiple joint military exercises to deter North Korea. Asian allies also cooperated with non-allies. India has

now become a key strategic partner of the United States and deepened its relations with other US allies. These events show that inter-alliance defense cooperation has become much more common, and the spokes have established tight connections with each other. Interactions between US allies and non-allies have also significantly increased. These activities have brought solid interoperability between the US, its allies, and its non-allied "strategic partners" during military operations.

Increased inter-alliance cooperation raises the question of whether allies of the United States in Asia will continue to strengthen their ties and eventually develop into a multilateral and institutionalized military cooperation. Possible forms of cooperation range from a treaty alliance to a defense agreement that coordinates defense strategies. The US is likely to take the lead in coordinating defense strategies among them, and even if such cooperation is organized by other allies, it is likely to take a key role due to its influence in regional security. Either way, the US is set to transform the current "hub-and-spoke system" into a multilateral institution. Even if a formal alliance were lacking, this institution would still coordinate ally-defensive strategies as they prepare for joint military operations in the future. Such a multilateral institution could also expand to include partners who have no alliance treaties with the US.

The revival of the Quadrilateral Security Dialogue (hereafter the Quad) points out the optimism for broader multilateral defense cooperation that includes both US allies and non-ally partners. The Quad was originally a multilateral disaster response initiative established by Australia, India, Japan and the US after the 2004 Indian Ocean tsunami. In November 2017, the four states met again and pledged to cooperate in defense and economic development. This meeting is usually referred as the Quad 2.0. Consisting of two allies and a strategic partner of the United States, this quadrilateral dialogue could lay the foundation for a multilateral alliance or a tighter mechanism of military cooperation. Former United States Pacific Command Admiral Harry Harris once stressed the importance of building regional security through quadruple defense cooperation (Harris, 2016). Some scholars and foreign policy analysts also hold an optimistic view about the role the Quad can play (Liu, 2018; Singh, 2018; Smith, 2018). Some anticipate that international structure would lead to closer security ties between East Asian countries. Chanlett-Avery and Vaughn (2008) paid attention to the emerging Asian trilateral ties in their report to Congress. Burgess and Beilstein (2018) argue that a multilateral defense pact is possible if China and North Korea become more aggressive. Lee-Brown (2018) also argues that a minilateral security community has already emerged over the past decade as regional countries have built an array of overlapping "security triangles." To be sure, these authors maintain that there are significant barriers to forming a multilateral

defense alliance, but they tend to agree that maritime security and the North Korea threat will at least incentivize the US, its allies, and its partners to establish closer defense cooperation if not a defense alliance.

This paper evaluates the prospects of a closer multilateral security partnership in Asia. In particular, it examines whether the US or its allies would support a multilateral institution in the Indo-Pacific region. Even if a treaty alliance seems far-fetched, how would the US and its allies alter the current hub-and-spoke system? Starting from the theory of alliance management, the following analysis examines alliance relations in East Asia since 2016. Evidence suggests that despite the increase of inter-spoke co-operation, a multilateral defense mechanism is unlikely to develop. The United States would remain a key player in regional security, and Asian allies welcome its involvement in regional affairs. However, Asian allies will find it difficult to resist the demands from the US when they disagree with the US over burden-sharing and overseas operations. This is due to the United States' bargaining advantages in the hub-and-spoke system and its desire to maintain oversight over its Asian allies and partners. The current hub-and-spoke system allows the US to prevent its allies from initiating collective bargaining while providing it with an advantage in burden-sharing negotiations.

This discussion begins with a review of alliance theory and its implications for the hub-and-spoke system by explaining why a stronger power is expected to enjoy more bargaining advantages in a bilateral alliance than a multilateral one. Next, it examines cases of burden-sharing disputes between the US and its allies. The issues discussed cover THAAD and US deployment costs, allied operations in the South China Sea and Indian Ocean, and arms sales to US allies. These cases show that allies sometimes have common grievances with respect to US demands, and such grievances are particularly salient under the Trump administration. US allies cannot jointly raise a complaint with the US but must instead negotiate separately. The US has made it clear that such problems are to be handled individually with each ally. Asymmetric power relations in a bilateral alliance also undermine the bargaining leverage of US allies. Allies find it difficult to resist US demands, and they are sometimes compelled to accommodate its strategic interests.

At the same time, the US has no incentive or need to establish dominant control over its Asian allies in a manner similar to the Soviet Union and its satellite states. Weaker American allies have room to pursue their foreign policy objectives, but such autonomy does decrease as the US requires more help from them to cope with regional security challenges. As China's military power and foreign policy influence increases, US allies are finding it increasingly difficult to remain neutral or exercise hedging

policies in a climate of US–China competition, and this is particularly pronounced in regional security issues.

Bargaining Power, Burden-Sharing, and Bilateral Alliances

States form security pacts as they face security challenges. They make careful evaluations of the value of alliances and the reliability of potential allies before forming a security alliance (Crescenzi, Kathman, Kleinberg, & Wood, 2012; Walt, 1987; Weitsman, 2004). Alliances are designed to create stability but sometimes impact the balance of power (Waltz, 1979).[1] They deter external rivals from launching attacks and restrain allies from taking risky moves. However, relations between alliance members are not always harmonious. Alliance members constantly worry about entrapment and abandonment (Snyder, 1997). They do not always have consistent perceptions of external threats; neither do they always agree on each other's foreign policies. Due to fear of entrapment, states often pay close attention to their allies' foreign policy moves and intervene when they believe these will violate their interests. States therefore set up institutions before and after alliance formation to prevent betrayal and opportunistic behavior (Leeds & Mattes, 2007; Narang & LeVeck, 2019). Such intervention includes efforts to assist the ally in achieving its foreign policy goals or to prevent the risky provocation of an ally (Benson, Bentley, & Ray, 2013; Kim, 2011).[2]

Members of an alliance therefore constantly manage their alliance relationships, which helps facilitate the cooperation established by the treaty. Alliance management aims to coordinate the divergent security interests of members, define and clarify treaty obligations, and facilitate substantive defense cooperation. The process of coordination is essentially bargaining between allies (Snyder, 1997, Chap. 6). Stronger members or primary security providers usually enjoy greater bargaining power. Minor states, on the other hand, tend to make more concessions on their autonomy in exchange for security (Morrow, 1991). In general, minor allies rely on the stronger ones for their security. This gives stronger allies an opportunity to create alliance

[1]The security alliances discussed in this article are treaty alliances with military obligations, namely offensive and defensive alliances. Treaties that denote neutrality or military consultation rarely require constant cooperation during peacetime. These alliances are beyond the scope of this paper. However, if a multilateral mechanism were to emerge in Asia, it would be likely to start with a formalized consultation mechanism. The Quad represents such a mechanism. The main question of the paper, therefore, is whether such mechanism will deepen or expand.

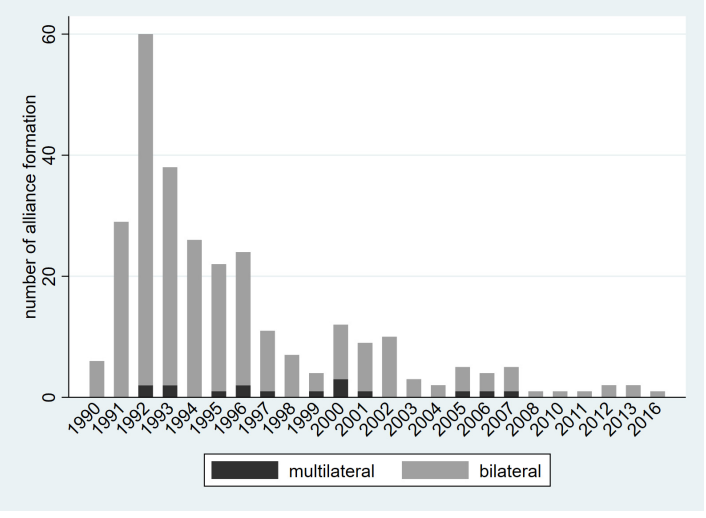
[2]Institutional design is a common method to manage intra-alliance disagreement, see Leeds (2003) and Morrow (2016).

relationships that are more accommodating to their interests. They can push institutional designs they deem appropriate (Mattes, 2012). They can also compel minor allies with the threat of a change to the nature of their cooperation, including the suspension of alliance obligations (Haftendorn, Koehane, & Wallander, 1999, Chap. 4).

Like any international cooperation, alliance cooperation is plagued with information problems and distributional concerns (Morrow, 1994b). Members of an alliance may disagree over forms of cooperation, and they may have different opinions about the security gains offered by the alliance. They tend to maximize security returns by offering the least resources they can spare. Since an alliance provides club goods shared by all members, free riding is a common concern that might jeopardize an alliance relationship. Stronger allies usually have little choice but to bear a disproportionate burden in an alliance because minor allies have a smaller marginal impact on joint security gains (Morrow, 1994b; Olson & Zeckhauser, 1966). This is especially true in a more institutionalized alliance (Morrow, 1994a). To avoid free riders, stronger allies usually force weaker members to contribute or follow foreign policy directions preferred by the stronger allies. Stronger allies punish disobedient ones by ceasing cooperation or by following a tit-for-tat strategy (Sandler & Hartley, 2001). Therefore, even though the burden-sharing is unlikely to be fair to the stronger allies, they are more likely to fulfill their foreign policy goals through their influence on the minor allies.

The bargaining power of a stronger member is more salient in a bilateral alliance than in a multilateral one. First of all, the number of players affects the efficiency of intra-alliance bargaining. Institutional theory posits that a large number of actors can impede international cooperation. A larger number of members increases the incentive to free-ride, resulting in an insufficient provision of collective efforts (Olson, 1971). As multilateral cooperation involves more divergent interests, it becomes more difficult to negotiate a cooperation arrangement that has been jointly agreed upon, and a group pays more transaction costs as the number of members increases. Great power support is usually key for successful multilateral cooperation because it can sustain cooperation as the great power pays extra costs (Krasner, 1983; Martin, 1992). Therefore, Oye (1985) argues that reducing the number of players produces more robust cooperation. Due to the high cost of alliance formation, multilateral alliances are relatively more difficult to form than bilateral ones. Among the 745 treaty alliances registered in the Alliance Treaty Obligations and Provisions project (ATOP 4.0), only 107 of them are multilateral (14%).

A survey of post-Cold War alliance formation also shows this trend. After the collapse of the Soviet Union, the newly independent Soviet Republics and Eastern



Source: Data compiled by the author, based on ATOP 4.0 (Leeds *et al.*, 2002).

Fig. 1. The numbers of alliances formed since 1990.

European communist states re-established their alliance ties. Instead of building multilateral alliances to accommodate their security interests in post-Soviet Europe, these states formed a large number of bilateral alliances in the early 1990s. Figure 1 shows about 95% of new alliance formations after 1990 were bilateral. To be clear, this number does not provide evidence of bargaining power within an alliance, neither does it prove that stronger powers prefer bilateral alliances. It does however indicate that bilateral alliances are easier to establish. States are inclined to create bilateral alliances because multilateral ones are harder to negotiate and harder to manage.

Building multilateral alliances can have several benefits. A multilateral alliance can facilitate the exchange of information, reduce transaction costs, and generate focal points for security cooperation. The multilateral setup in general helps to organize an effective deterrent signal against external threats. However, a multilateral scenario does not necessarily help to manage internal differences between allies. Alliance management in a multilateral alliance is essentially about commencing several bilateral negotiations at the same time in which the response of each member affects the bargaining strategy of the others. If a distributional problem occurs (financial contributions to the alliance, for example), it is likely to be more complicated and more difficult to resolve in a multilateral alliance than a bilateral one. The greater the number of allies in an alliance, the more divergent their interests are. Allies are usually compelled to spend more time and effort to settle their cooperation.

More importantly, multilateral negotiations allow members to resist demands from other members. This often occurs when the security providers in the alliance who usually are the stronger members have divergent interests from other minor members. Consider a simple scenario where one ally is much stronger than the others and acts as the main security provider in a multilateral alliance. Other minor members offer their military capabilities, raw materials, and key transportation sites to the alliance. When the stronger member requires minor members to perform certain tasks to advance common security interests, some minor members may argue for alternatives.[3] Their disagreements are based on common reasons that may occur in any alliance: They may disagree with what the common defensive interests are, believe the distribution of responsibilities is unfair, wish to free-ride while others contribute, or feel concerned that the stronger member will make more demands in the future. In a bilateral setting, it usually comes down to who has more bargaining leverage over the other. The available bargaining leverage in a multilateral setup makes intra-alliance bargaining more complicated.

Since there are more members in a multilateral alliance, minor allies tend to compare their burdens with one another. They are likely to use the terms given to other minor allies as leverage during their bargaining with the stronger ally. They may argue that they bear unequal responsibilities or that other allies are more fitted for such responsibilities. They can also delay their efforts, arguing that it is due to coordination problems with other allies.

Another problem is that a coalition of resistance may emerge within a multilateral alliance. This can be either a coordinated or uncoordinated effort. Minilateral cooperation is an example of the former. An alignment with some members within a larger organization reduces transaction costs and minimizes the divergent opinions within that small group (Kahler, 1992; Snidal, 1985). At the same time, it also provides an opportunity for members to coordinate a common position during negotiations. Depending on the institutional design, a group of minor members may have better bargaining leverage in multilateral settings. The Group of 77, for example, successfully pushed for their economic development agenda in the United Nations. In security alliances, minor members may coordinate their bargaining strategies against

[3]Minor members do not necessarily resist the stronger member's request. If all members agree with the stronger power, there will be no intra-alliance bargaining and members can easily cooperate. There is no difference between multilateral and bilateral alliances in this case. However, when one or more minor members disagree with the stronger ally, they will bargain with each other.

the stronger ally.[4] A coalition of minor allies can engage in collective bargaining with the stronger members. As a group, they will enjoy better bargaining leverage than when responding to the stronger ally alone, as they have more opportunities to make issue-linkages based on their various security interests.

An uncoordinated response is an unintended consequence of minor members. A minor member may choose not to cooperate with the stronger ally, and its resistance prompts other minor allies to follow. A minor member may claim that it will cooperate only if another member agrees to. It may also withhold its contribution when it observes that other members do not cooperate. Although each member makes its own decision, these decisions are implicitly linked to form a joint response. The stronger member finds it more difficult to negotiate with such a coalition because a common position is lacking among minor allies. The strong member may have to tailor its demands to each minor member and persuade them individually.

Whether or not their responses are coordinated, minor members can form a coalition against the stronger ally that makes it difficult for the ally to punish minor allies. Sanctioning an uncooperative minor member may cause a collective response from other members. Sometimes sanctions only push minor members to cooperate more closely because they are aware that they cannot resist the stronger member separately. The resistance of minor members may paralyze the alliance and force stronger members to concede. The problem is more acute in multilateral alliance because minor members have an opportunity to form such coalitions. In bilateral alliances, the minor ally already has poorer bargaining leverage due to its weaker capabilities. It also lacks the opportunity to link its security benefits with a third country. Even if a minor ally controls strategically important territories or resources, its policy autonomy concerning the sharing of these assets can be hampered by its dependence on the stronger ally.

NATO's burden-sharing dispute provides an example. Minor members resisted a dominant ally by delaying their actions, and the dominant ally could not effectively compel the minor members. Burden-sharing has always been a struggle between Atlantic allies and has dominated NATO's agenda in recent years. At the 2017 NATO

[4]It is true that some members may form another alliance to advance their own security interests. This is rarely a negotiation tactic to compel or threaten the stronger power in the existing alliance but rather a careful decision to fulfill their security needs. A new alliance does not necessarily compete with the existing one. If there is competition, the newer alliance usually better represents the updated security interests of the members, and the function of the existing alliance is likely to be replaced by the newer one. For example, the Western Union was established to deter German aggression immediately after WWII. Its function was soon replaced by the North Atlantic Treaty Organization (NATO), which provided much better security for its members. For how bilateral cooperation can enhance multilateral cooperation, see Verdier (2008).

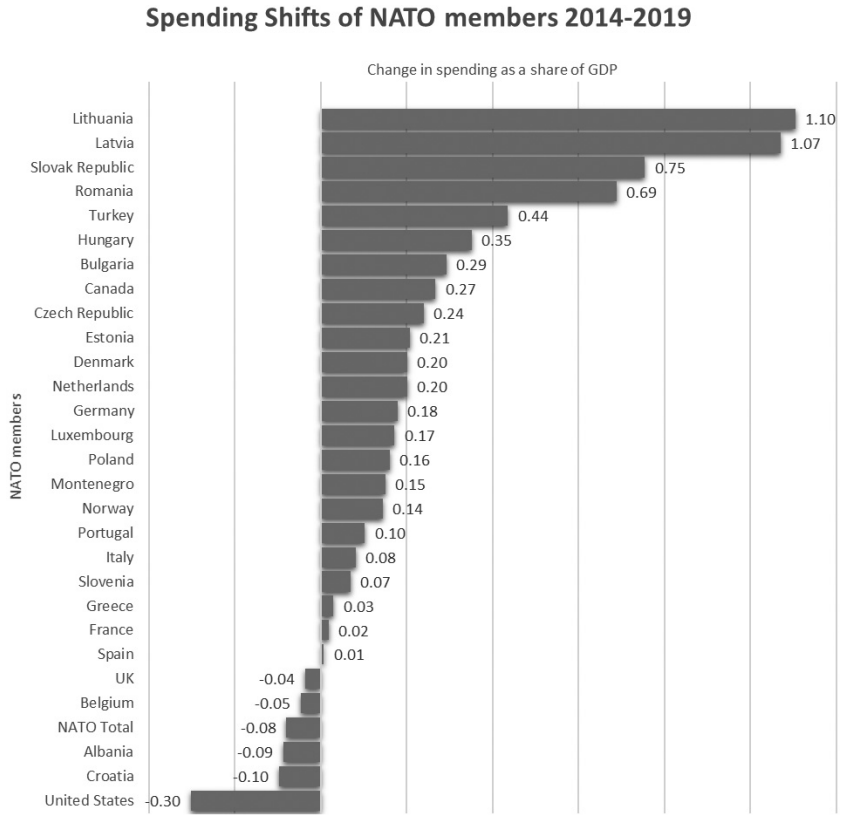
summit, President Trump publicly urged NATO members to increase their defense expenditures by 2% of their gross domestic product (GDP), setting a guideline for the individual responsibility of members for defense investment. He warned NATO allies rather bluntly: "This is not fair to the people and taxpayers of the United States."[5] Yet, after several rounds of minister and leader meetings, only six European allies met the 2% threshold in 2019, including Britain.[6] As Figure 2 shows, the sharpest increase of defense expenditures occurred among Baltic and former communist countries, who faced threats from Russia due to their geographic proximity. Similarly, three countries hit the target because they already had laws requiring their respective governments to spend at least 2% of GDP on defense.[7] Major NATO powers such as France and Germany, however, barely increased their defense expenditure. This example shows that the stronger member does not always get what it wants. The United States enjoys a dominant role in NATO due to its being the primary security provider, its bargaining power should be the strongest among the allies, and the Trump administration has repeatedly made clear and coercive demands in public. Yet, in spite of these factors, the US was still unable to compel major NATO allies to reach this threshold.

Despite Trump's strong words to pressure his NATO allies, they still chose to delay their actions or simply ignore American demands. Figure 3 shows estimated number of 2019 defense spending of NATO members. Germany, for example, significantly increased its defense expenses in 2019 by 11%, but it still fell behind the 2% target (1.36%). The US warned Germany that it would relocate American troops to Poland if Germany would not increase its defense spending. Instead, the German government insisted on cutting spending for the following years (Bennhold, 2019; Kitschbaum, 2019). The German government later formally pledged to reach the 2% goal by 2031, which is still far behind the 2024 deadline set by NATO allies (Emmott, 2019). Similarly, the French Minister of the Armed Forces said that European countries would make autonomous decisions on increasing their burden share. This echoed French President Macron's earlier proposal which urged European countries to establish a more autonomous security institution (Macron, 2019; Noack & McAuley, 2018). To be sure, NATO's European members did not collaborate on this matter. Germany and France did not join hands; neither did they call upon other NATO European allies to join in a boycott. They simply shared the position that the 2%

[5]See the remarks by President Trump at NATO (The White House, 2017). The 2% guideline was proposed in 2006 and reaffirmed in 2014.

[6]Lithuania's defense expenditure was very close to 2%. By another standard of calculation, Lithuania spent more than 2% of its GDP.

[7]These countries are Romania, Poland, and Latvia.

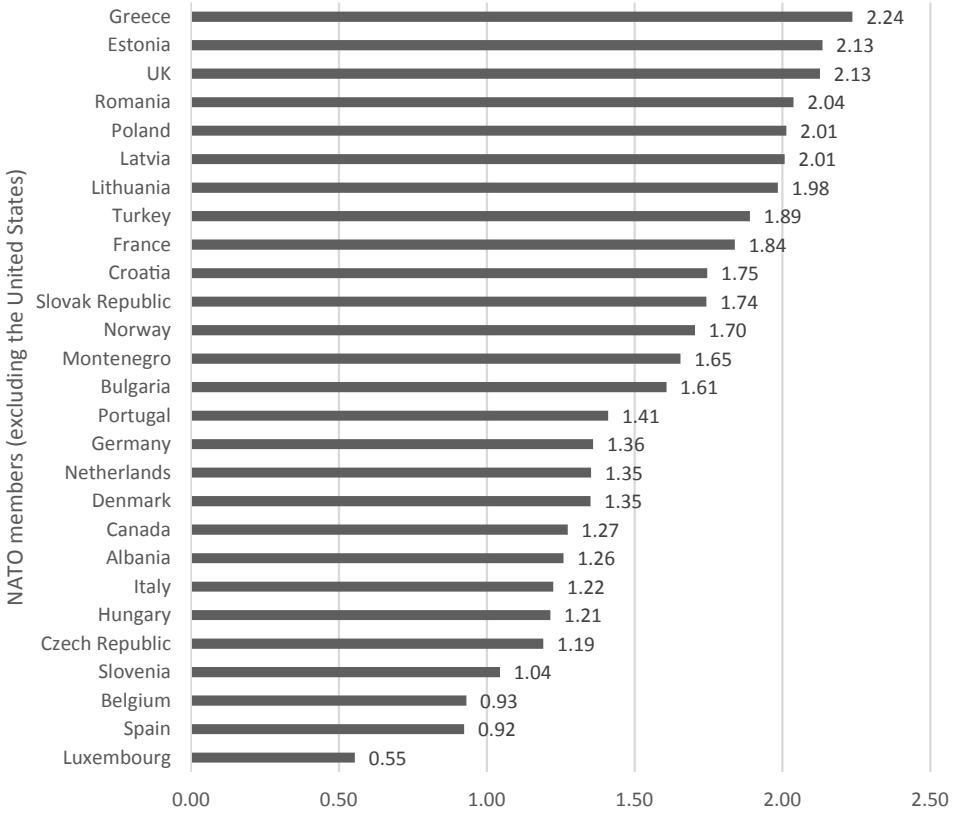


Note: The numbers for 2018 and 2019 are estimated by NATO.
Source: NATO (2019).

Fig. 2. Defense spending shifts of NATO members from 2014 to 2019.

goal was an unreasonable demand and expressed their objections publicly. This uncoordinated resistance proved to be effective when a majority of NATO members failed to provide plans to increase their defense budgets, and have so far suffered no consequences.

The resistance of NATO members presented a dilemma for the US. If the US sanctions NATO allies who do not meet the threshold, all alliance members will suffer the consequences of low cohesion in the alliance. It might also paralyze alliance cooperation and send a weaker deterrence signal to Russia. The countries who directly face Russian aggression would be concerned about discord among major NATO members and might request the US to settle its differences with non-compliant members. In other words, the US could not effectively punish free-riding behavior without harming the interests of other well-behaved members. While the US would



Source: NATO (2019).
Note: The numbers for 2018 and 2019 are estimated by NATO.

Fig. 3. The 2019 NATO members' defense spending as a share of GDP.

certainly not expel these members for failing to reach the 2% threshold, such discord would still hurt the alliance. The US lacks the leverage to coerce these states, especially when they do not feel an imminent security threat as other members do. On the other hand, when the US rewards Baltic and Eastern European allies by bolstering their defenses, all other members benefit from a more robust deterrence against Russia, and non-compliant NATO members still enjoy a more secure Eastern border. This example shows how hard it can be for a strong or even dominant ally to force others to act. Allies can ignore pressure from the dominant power because it is difficult to punish multiple allies who refuse to cooperate.

A stronger ally can employ stringent controls in a multilateral alliance. If this ally is deeply concerned that minor allies might abandon the alliance, its desire to control the minor allies may lead it to create a hierarchical alliance. The satellite states of the

Soviet Union, for example, were tightly subjected to Moscow's informal empire. The same principle applied to US dominance in the Caribbean Sea (Lake, 1996). Hierarchical alliance relations leave very little policy autonomy for minor allies and give them no leverage to advance their own interests. The dominant ally expends significant resources to ensure the allegiance of its protégés. Soviet military intervention in Hungary and Czechoslovakia demonstrated how costly this alliance management method can be. If a stronger ally is determined to pay such costs to dominate its ally, there is little room for intra-alliance bargaining and therefore no significant difference between bilateral and multilateral alliances.

Nevertheless, alliance relations in the post-Cold War era have been much less hierarchical. Alliance members constantly adjust their military cooperation and renegotiate burden-sharing arrangements. The rise of the number of defense cooperation agreements since 1990 shows that alliance members often negotiate their security relations. These agreements deal with military exercises, arms sales, logistical support, defense technology transfers, and intelligence sharing (Kinne, 2018). This trend suggests that intra-alliance bargaining has been much more frequent. Disagreements, persuasion, and inducement have become common in alliance relations. Material capability remains a key indicator of a member's bargaining power. Minor allies who do not make fundamental contributions are subjected to pressure from the stronger ally. Their policy autonomy is constrained, and their security policies usually need to accommodate the strategic interests of the stronger member.

In sum, allies each have their own interests and attempt to convince their members to accommodate them. Sometimes they coerce allies in order to achieve their foreign policy goals. The stronger ally is likely to enjoy a bargaining advantage in intra-alliance bargaining. As they usually take on a greater share of the defense burden, the security they offer becomes their bargaining leverage. Therefore, they are able to interfere with the foreign policies of minor allies. However, this advantage is not as salient in a multilateral alliance as in a bilateral one. A stronger ally suffers several disadvantages within a multilateral institution: divergent interests make it difficult to accommodate every member. Minor allies can also unite to increase their bargaining power. In bilateral bargaining, the stronger ally finds it easier to exert influence over the minor ally, even though the stronger ally must bear a greater burden. The stronger ally thus has few incentives to form a multilateral alliance or combine several bilateral alliances into a multilateral one. Furthermore, the stronger ally will prevent any coalition between minor allies under multilateral cooperation because such a coalition may harm its bargaining power. It will also obstruct coordination between minor allies in different bilateral alliances.

The Iron Spokes

How do these theoretical propositions apply to the alliances of the United States in Asia? While these bilateral alliances were established in the wake of World War II when the US aimed at deterring the communist threat, their function has changed since the end of the Cold War. The US uses the system to coordinate the actions of its Asian allies while maintaining its influence over each. Keeping the cooperation bilateral strengthens the bargaining leverage of the United States when it makes demands on allies. As the diverging security interests of America's Asian allies also give it an advantage, the US provides different cooperation arrangements to cope with their differing security concerns. It therefore makes different demands on each ally and asks for different contributions in return.

There is no doubt that the US has enjoyed a bargaining advantage in East Asia, and alliance relations have been quite close. However, there are two recent developments in the region that have altered the relations between the US and its allies. First, the US has felt an increasing security challenge from China. US–China competition in the South China Sea is among the most serious disputes faced by either side, and all US allies are affected. North Korea represents another threat that is leading the US to strengthen defense strategies with its allies. Second, as Trump carried out his "America First policy," the US took initiatives to request significantly more contributions from its Asian allies. These developments created more opportunities for joint operations while also creating more incidents of intra-alliance bargaining.

It should be noted that the US always plays a key role in East Asia. It has a significant impact over regional economic development, political stability, and security. However, a series of new developments in Asia prompted Washington to review its Asia policy, and it subsequently decided to divert more resources to Asia. The catalyst of this heightened security concern began when China made military provocations around the Senkaku/Diaoyu Islands and its later expansion in the South China Sea. To cope with these security issues, the Obama administration proposed a "Pivot to Asia" that has been widely referred to as a "rebalancing" strategy. Under rebalancing, the US devoted more diplomatic effort and resources to the Asia-Pacific region (Lieberthal, 2011).[8] In the security realm, it reinforced and strengthened its military cooperation through its hub-and-spoke alliances. The US redeployed military assets in

[8]Obama's rebalancing or "Pivot to Asia" is a comprehensive engagement strategy. In addition to security, pushing economic relations, joining disaster relief, and establishing people-to-people contacts were all part of Obama's rebalancing. For the details of its rebalancing strategy, see Manyin et al. (2012) and Tow and Stuart (2014).

Asia that included both land and naval forces in the Pacific. US forces regularly held joint military exercises with its allies. US naval activities in the South China Sea became more active as China toughened its claims in the area. The US also reached out to non-allies, building closer security and economic relations with the Philippines, Vietnam, and India. As a whole, the rebalancing strategy did not seek to resolve imminent security threats but to prepare for challenges that might arise in the future.

The use of multilateral institutions in fact played a key part in Obama's rebalancing. The US accelerated negotiations for the Trans-Pacific Partnership (TTP) agreement, strengthened relations with Southeast Asian countries via the ASEAN Regional Forum (ARF), participated in the East Asia Summit (EAS), and supported dialogues and military exercises coordinated by the ASEAN Defense Ministers' Meeting-Plus (ADMM-Plus).[9] The US gave full support to multilateral diplomacy and sought critical influence in those forums. Although the Obama administration embraced the multilateral mechanism to boost cooperation between allies and non-allies, the rebalancing relied on the existing bilateral alliances when it came to regional security. An overview of Obama's security policies toward allies in Asia shows that the US engaged with each to strengthen its military presence. For instance, it continued to discuss the relocation of the Futenma airbase with Japan. It carried on negotiations with the South Korean government to move American troops to a new base in Pyeongtaek.[10] In 2014, the US signed the Enhanced Defense Cooperation Agreement (EDCA) with the Philippines, granting it access to military bases.

These efforts either sustained or expanded America's presence in Asia while remaining strictly bilateral. The Obama administration partnered with specific allies to face each regional security challenge: The US joined hands with South Korea after the sinking of Cheonan and the Yeonpyeong shelling, backed up Japan in a territorial dispute in the East China Sea, and deepened engagement with Vietnam during a dispute with China over the South China Sea. While the US played a major role in each crisis, it did not coordinate multilateral responses to them. It did not propose any multilateral security forum or dialogue between its allies as it had done in advocating the TPP or ARF. In terms of its alliance relationships, the US maintained the hub-and-spoke system while further consolidating its ties with each spoke.

Trump's Asia policy bears a certain resemblance to Obama's rebalancing. The US has continued to increase its presence in the region through military training,

[9]ADMM-Plus is a multilateral security dialogue established under ASEAN. It has hosted several multilateral maritime operations between the Asian countries. The US took an active role in ADMM-Plus. The author thanks the reviewers for their comment on this important development.

[10]The new headquarters of the United States Forces Korea at Camp Humphreys opened on June 29, 2018.

exercises, arms sales, and forces stationed in ally territories. Meanwhile, it established dialogues with non-allies such as Vietnam and India. The US has criticized China's fortification efforts in the South China Sea and challenged its territorial claims through naval operations. However, Trump's withdrawal from the TPP shows that he has downplayed the role of multilateral forums that Obama valued. Trump prefers to project American military strength and foreign policy influence by engaging with East Asian countries separately.

While US allies in East Asia have played a significant role in this process, the Trump administration has sometimes adopted unilateral measures. For instance, the change from "U.S. Pacific Command" to "U.S. Indo-Pacific Command" showed the county's intention to include South Asia in its strategic thinking. It opens the possibility of including partners in the Indian Ocean, though its allies were not consulted on this matter. Nor did they know how this might change American military activities in the Indo-Pacific region. Under the FOIPS, the US alliance management policies experienced a shift to echo Trump's catchphrase of "America First." The hub-and-spoke system has served as a portal for the US to accomplish its strategic goals. The US has asked its allies to host its forces, enhancing its ability to intervene in regional security issues. The US asked its Asian allies to contribute to joint operations and demanded that allies share a significant amount of the financial burden of maintaining a US military presence. It has also not been shy about expressing discontent toward free riders, demanding returns that consolidate American interests. The following discussion briefly shows how the US puts pressure on its three main allies of South Korea, Japan, and Australia.[11]

The US–ROK Alliance

The US demands have usually centered on burden-sharing and countering China in the South China Sea, and South Korea has experienced both pressures from Washington. Under Trump's urging that South Korea should bear more of the expense

[11]The Philippines is not included despite the fact that it is a treaty ally. The US–Philippines alliance is different from others, and its importance in the hub-and-spoke system is declining. The US has not relied on the Philippines to project military power since the closure of Subic Bay. The military relations maintained during the War on Terror and the 2014 EDCA authorized the US to access military bases. However, their defense cooperation was narrow and often issue-specific. US forces are no longer stationed in the Philippines. In recent years, alliance relations have suffered from the deterioration of relations between the Philippine President Duterte and the US government. Duterte recently terminated the Visiting Forces Agreement (VFA), which set the legal basis for the US to participate in joint military exercises in the Philippines. The Philippines therefore does not have the same importance as the allies discussed in this paper.

for American troops stationed on the Peninsula, the US and South Korea began strenuous negotiations in March 2018. After 10 rounds of failed negotiations, only a provisional arrangement could be reached, requiring that South Korea be responsible for half of the total cost (Choe, 2019). The US also asked South Korea to share the cost of deploying strategic assets such as aircraft carriers, submarines, and bombers, which the South Korean government firmly rejected ("S. Korea Rejects," 2018). The US asked South Korea to pay for the deployment of the THAAD system (Macias, 2018), and it is still unclear whether it has paid off the expense.

The US has sought to involve South Korea in defense responsibilities outside the Korean Peninsula and repeatedly asked that it became involved in the South China Sea. Trump's former defense secretary, James Mattis, publicly called on allies to "join[ing] hands together" against China's militarization in the South China Sea (Axelrod, 2018). The South Korean government under the progressive President Moon Jae-in was reluctant to answer such a request (Panda, 2019). Facing a direct threat from the North, the South Korean forces have rarely joined military operations outside Northeast Asia, but its navy joined the US-led Pacific Vanguard Exercise along with Japan and Australia in 2019. This was the first joint navy exercise near Guam involving all allied forces. Despite strained relations between South Korea and Japan, South Korea joined the drill after a US request ("S. Korea, Japan," 2019). The exercise aimed to improve the interoperability of allied forces in the Indo-Pacific region rather than deterring North Korea.

Although there is no clear evidence that the US requested South Korea to take part in its Freedom of Navigation Operations (FONOPs), the South Korean navy has shown support for its efforts in the South China Sea. Claiming to be dodging a typhoon in September 2018, a South Korean anti-piracy warship sailed within 12 nmi of a land feature occupied by China (Page & Jeong, 2018). China issued a protest and South Korea made no comment on its passage. The US issued a statement signaling its full support for South Korea's right to freedom of navigation. In July 2019, President Moon publicly endorsed Trump's Indo-Pacific strategy (Jung, 2019). Although the Blue House did not confirm, it is assumed that Moon might have made this decision under the US pressure (Lee, 2019). The shift of South Korea's support to operations in the South China Sea and endorsement of FOIPS suggests that US demands were effective, and South Korea has echoed American strategic interests despite its initial reluctance.

The US–Japan Alliance

As the United States' ironclad ally and home for its forward bases in Asia, the US–Japan alliance plays a crucial role in US power projection there.

Unlike South Korea, the Abe government has been more willing to comply with American requests. Japan has been wary of the rise of China due to the Senkaku/Diaoyu Islands dispute. China's move to cut the supply of rare-earth minerals in 2010 made Japan concerned about the country's use of economic statecraft (Inoue, 2010).[12] Countering China's territorial claims in the South China Sea may also help Japan in its own territorial dispute with China. Similarly, joint military operations with the US have helped Abe to achieve his political agenda. Since his inauguration, Abe has been striving toward the normalization of Japanese forces through a revision of the country's constitution. Changes to Japan's security laws in 2015 allowed the SDF to participate in overseas missions. Abe needed American support to counter criticism of Japan's remilitarization from its neighbors as well as from opposition parties. The JMSDF subsequently began regular overseas operations after the security law revisions.

Japan has been a regular participant in joint military exercises with the US, and two developments have been notable in recent years. The first is Japan's presence in joint exercises with America's partners. Japanese personnel have participated in the biannual Talisman Sabre exercise involving the US and Australia since 2019. Its newly established marine unit performed an amphibious landing during the first exercise (Gady, 2019). Japan also partnered with India to conduct military exercises in the Indian Ocean. Since 2015, Japan has become a regular participant in the US–India Malabar naval exercise. Since 2013, India and Japan have conducted the bilateral exercise JIMEX, though India is not Japan's only military exercise partner in South Asia. The Japanese Izumo-class helicopter carrier recently conducted an exercise with the British Royal Navy in the Indian Ocean (Kelly, 2018).

The other development is Japan's presence in the South China Sea. Although it did not join the United States in FONOPs, the country's military cooperation with Southeast Asian countries has nevertheless become more frequent (Bao, 2016; "Japan Supports," 2017).[13] Japan conducted various naval exercises with the US in the South China Sea and the Philippine Sea (The U.S. Navy, 2019). A Japanese submarine participated in one of the exercises, signaling an unprecedented projection of power since the end of the Second World War. Japan's Izumo-class carriers have regularly sailed to the South China Sea to participate in naval drills with the US, Australia, and India. They have also made port calls at claimant countries in the South China Sea.

[12]China did not ban rare-earth exports to Japan but stalled shipments by bureaucratic procedures. The volume of trade was not impacted by this brief halt, but this action certainly alerted Japan.

[13]Since 2016, Japan has declared that it would not join FONOPs. The Japanese government has not changed this position.

In 2019, Japan sent its JS Izumo helicopter carriers (Johnson, 2019) to participate in an exercise with the US, India, and the Philippines. This was the most significant show of force in the South China Sea in recent years. Japan also explored relations with non-allies in the South China Sea. Abe promised to supply patrol boats to Vietnam during his visit in 2017 (Nguyen & Pham, 2017).

Japan procured F-35 stealth fighters and confirmed more purchases of the F-35B in 2019.[14] The purchases were clearly a response to Trump's criticisms of Japan's free-riding behavior. Trump allegedly mused about ending the US–Japan alliance because the relationship was unfair to the US (Jacobs, 2019), and the Abe administration seemed to heed this latent threat. It took a swift action to improve its share of the burden, something that allies in Europe had failed to do. In addition to the overseas operations mentioned above, Japan significantly boosted its defense expense by 1.2% (Kelly, 2019).[15]

The US–Australia Alliance

Like Japan, Australia has increased cooperation with the US in order to defend its security interests in the region. Since 2016, the US has requested that Australia join its Freedom of Navigation Operations (Johnson, 2018; Joshi & Graham, 2018). Australia has demurred while still following a policy of protecting its right to freedom of navigation. Since 2016, Australia has been concerned about China's military activities in the South China Sea and has adjusted its defense strategy to cope with this security challenge (Schreer, 2016). The Royal Australian Navy (RAN) often sails through the South China Sea, though it does not cross the 12 nmi line as the US does. More recently, RAN operations have been clearly intended to deter China's military activities in this region. In 2018, three RAN vessels transited through an area in the South China Sea where the People's Liberation Army Navy (PLAN) conducted its largest naval exercise. The Australian vessels received warnings from PLAN, but Chinese vessels did not interrupt their transit (Wen & Paul, 2018). Australia also deepened its strategic partnership with India based on the 2009 Joint Declaration on Security Cooperation. Under this agreement,

[14]The F-35B purchase is important because it is a short take-off and vertical landing (STOVL) aircraft. Japan will be able to land F-35Bs on the Izumo-class carrier. With the purchase of 105 F-35A and 42 F-35B models, Japan will establish the largest F-35 squadron outside the US. The country recently expressed an interest in becoming an "official partner" for the F-35 program. The Pentagon rejected Japan's request. See "Japan Formally" (2019), Mehta (2018), and Mehta, Insinna, and Yeo (2019).

[15]Note that the surge was largely due to the F-35 purchase.

Australia conducted biannual naval exercises (AUSINDEX) with India since 2015 ("India-Australia Joint," 2019).

Australia has been willing to support American military operations in the region, but it has refused to join direct confrontations against China. Nevertheless, the country's alliance ties with the US have drawn China's attention. In 2019, a Chinese warship tailed RAN vessels during their transit through the South China Sea (Martin, 2019). Australia's concerns over the rise of Chinese power have made it more willing to facilitate a US military presence in the South Pacific. For instance, Australia has planned a new deep-water port to host more US marines. If completed, this new port is likely to significantly increase the US military presence in the South Pacific when compared to the current US marine rotation in Port Darwin (Greene, 2019).

Do Personal Traits Explain the US Alliance Management in Asia?

The three allies significantly increased defense cooperation with the US at the request of Washington, but frictions over burden-sharing have also arisen. As the US increases its demands on allies, allies have sometimes resisted or tabled the issues. It is often believed that the policies of President Trump were the fundamental cause of friction with Asian allies. It is also argued that a different president would not create such tensions. It is true that Trump and his advisors have not been shy about asking allies to shoulder more responsibility. Trump often laments in public that military deployments in Japan and Korea cost too much, and his advisors shared these views. It was reported that the former National Security Advisor John Bolton asked allies to increase their share fivefold when he visited Asia (Jo, 2019).

However, disagreements with allies may still occur even if Trump had not taken a more coercive position regarding burden-sharing. To be fair, the Trump administration faces a more stringent geopolitical challenge than its predecessors. The rise of China both militarily and economically has alarmed Washington as well as its Asian allies. The heightened North Korean threat and South China Sea disputes require the US to mobilize its allies and build closer defense relations. Such cooperation would require Asian allies to take a greater role in regional defense. The costs of cooperation increase as joint operations become more frequent. The US would have asked allies to bolster their defense capabilities, which would imply greater financial commitments. Although a different president would not focus on the financial contributions of allies as Trump did, the US would still require the allies to make more substantive defense contributions.

Regardless, the alliance relations discussed above show that the US was more capable of pressuring its Asian allies than pushing its European ones.[16] The US was not able to push some European allies to contribute as it wished, but it was able to push all three allies to publicly express their support for its position in the South China Sea disputes. The US was also more successful in asking for financial contributions from its Asian allies. It enjoyed better bargaining leverage in each bilateral alliance relationship. Each Asian ally has its specific security needs, and while the US has largely met them, it has also asked allies to accommodate American interests. Even if an ally is dissatisfied with US security provisions such as in the case of South Korea, it cannot simply ignore the country's requests. Korea and Japan both have an interest in pushing the US to counter the threat of North Korea, but they were unable to effectively compel the US on this matter because the US would not discuss with them in a multilateral setup. The US managed the two alliances separately and gave these allies different security guarantees. Both allies made contributions and gave policy support to the US. The US provided specific defense solutions with each of them while accomplishing its strategic goals in the process. Meanwhile, both countries must struggle with greater demands from the Trump administration.

US Oversight of Inter-Spoke Activities

Although the Asian allies of the United States have become more connected in recent years, they do not have the autonomy to choose what they can work on or with whom they can work with. Upon examination, minilateral cooperation between America's allies and partners has entirely been under the close oversight of the US. For example, the engagement between India and its allies in Asia was the result of US coordination. The US declared India a "major defense partner" in 2016 (Gould, 2016). The country has not only deepened cooperation with India in every aspect, but also has encouraged its allies to increase the defense cooperation with India as part of the FOIPS. As a result, the US introduced India to its allies and has pushed for inter-alliance cooperation. India has increased military drills and expanded economic exchanges with America's allies. South Korea's "New Southern Policy" corresponded to a call of the United States for cross-Indo-Pacific cooperation.

[16]European allies are in general more capable of resisting the requests of the US than its Asian allies. France and Germany are rich countries with strong armed forces. In addition, Western European countries do not directly face threats from Russia. As mentioned in the previous section, the Baltic and East European countries are more willing to follow the demands of the United States since they face a threat from Russia.

America's allies have responded to US demands to safeguard common security interests in the Indo-Pacific. As mentioned above, Japan has played a more active role in the Indo-Pacific, connecting all US allies and partners with military exercises and arms procurements. To be sure, Japan had already engaged with other regional middle powers such as Australia and India. Its vigorous engagement showed its anxiety about China's rise. When the Trump administration increased the US military presence in Asia, Japan faithfully followed the US to the South China Sea and the Indian Ocean. The helicopter carrier JS Izumo has regularly sailed through the South China Sea, making port calls at America's allies and partners. The JMSDF vessels participated in joint exercises held by the US in Southeast Asia. Close cooperation between Japan and the US suggests that the US has played a leading role in Japan's overseas maritime operations.

To be clear, Japan has an incentive to send its navy vessels overseas in order to secure more security partners in its competition with China. However, JMSDF joint operations with the US, Australia, India, and the Philippines were a coordinated effort of the US, and the exercises accommodated US security needs. These operations took place in the Sea of Japan, the East China Sea, the South China Sea, the Indian Ocean, and near Guam. Essentially, JMSDF sailed into places where it did not have vital interests. Japan increased its security relations with Australia and India because it was willing to accommodate American strategic interests. The operations contributed less to Japan's core security interests, but significantly helped the US strengthen its defense cooperation with regional allies and partners. For example, without the encouragement of the United States, Japan would not have been interested in selling patrol boats to Vietnam or in holding exercises with the Philippine Navy. Japan's assistance to US partners and joint naval exercises with India helped the US challenge China in the South China Sea, showing its resolve to secure freedom of navigation there. Although the US was not directly involved, Japan's assistance helped it to strengthen its relations with non-allies in the dispute.

Japan was not the only ally who expanded partnerships with non-allies under US encouragement. Australia also stepped up its exchanges with both allies and non-allies. In addition to Japan, Australia has sought military cooperation with India. India and Australia have conducted three AUSINDEX, with each exercise larger than the previous. The US has also played a role in these exercises. American and New Zealand military personnel were onboard an Australian vessel to observe the 2019 AUSINDEX (Ministry of Defence, India, 2019a,b). American participation suggests that the US kept a close watch on its allies. It chose to become involved not because it was concerned that allies might collude against it, but to ensure its allies and partners

could operate together, making them capable of assisting its strategic goals in the region.

There are few, if any, spontaneous instances of military cooperation between America's allies, and almost all military cooperation between allies occurs under the oversight of the US. Allies rarely need to approach each other without US encouragement. For instance, although both South Korea and Japan both face a threat from North Korea, they have rarely proposed joint military actions. This lack of incentives is largely due to historical and ongoing territorial disputes. Nevertheless, North Korea has been a genuine threat to both countries, and it would seem prudent that they at least discuss their strategy toward Pyongyang's missile tests. Yet the two governments have had no such joint actions or policies against a common external threat. Indeed, the presence of American forces in Northeast Asia has allowed the two countries to avoid seeking cooperation over North Korea. The US took the responsibility to defend its allies and prepared contingency plans for the event that any allies were attacked. Japan and South Korea chose to consult the US regarding their defense instead of their neighbors, lacking the incentive to discuss joint defense policies unless requested by the United States.

Australia was also encouraged to strengthen relations with other Asian allies and distribute resources to areas that were not among its core interests. While Australia cares about security in the South China Sea and its influence over Pacific Island nations, it did not seek to collaborate with other US allies over these issues. Australia is more interested in partnering with Pacific Island nations to hold sway in the South Pacific. The country has an interest in peace in the South China Sea as it is a vital trade route, but it is not a claimant in any disputes. Its policy has been to encourage dialogue between disputants and to stop the reclamation of the occupied islands while avoiding direct involvement. Australia has little interest in coordinating defense with other US allies and partners to challenge China in the South China Sea.

However, Australia has started cooperation with India and Japan, and its warships have made frequent trips through disputed waters. Without an introduction from the US, Australia would not have been interested in securing the Indian Ocean by participating in AUSINDEX. Without US participation, it would not have attended the Malabar exercise. Without the American advocacy, Australia and Japan might not have as many joint military exercises as they do today. The US plays an important role in all inter-alliance cooperation, consolidating its inter-alliance security network over the past few years. The country's efforts have been very successful, making the best use of its bargaining advantage in each of its bilateral relations.

Multilateral Cooperation Based on the Quad?

If the US has been active in supervising its allies and partners to create a security network in the Indo-Pacific, it is worth discussing whether the US or its Asian allies are interested in building a multilateral security organization. As mentioned earlier, some analysts expect that the Quad can become a multilateral mechanism that specifically focuses on coordinating defense strategies against regional threats. With the United States, its two significant Asian allies, and a regional great power in South Asia, the Quad is composed of four major powers in Asia. Strengthening the organization may be an opportunity for further defensive cooperation that can deter regional security challenges. More importantly, the Quad has set an example of formal cooperation between the US allies and non-ally partners over security affairs. It may incorporate South Korea, Vietnam, or the Philippines in the future. A multilateral mechanism would set up closer communication channels and military interoperability that paves the way for a security alliance. It also helps project US capabilities across the Indo-Pacific region, giving it access to facilities there.

Japan had been a vigorous proponent of the Quad, seeking to build a "democratic security diamond" in Asia (Abe, 2012). It tried to revive the Quad because the Trump administration had not proposed an Asian policy it desired. The US then responded with a positive gesture of support, pledging to coordinate common objectives and initiatives through this security dialogue (Tillerson, 2017). However, its interest in the Quad quickly faded after the 2017 meeting. The Quad was not a key component of Trump's Asia policy; neither did the administration support its expansion. Demonstrating how the US perceived the Quad, the then United States Secretary of Defense Mattis did not mention the organization in his speech at the 2018 Shangri-La Dialogue. When Mattis was interviewed later by International Institute for Strategic Studies (IISS), he admitted that the Quad was in his original speech but had been cut to reduce its length (Chipman, 2018). As much as Mattis paid attention to the Indo-Pacific, the Quad was not his priority in the US defense strategy.

The US has few incentives to push the development of the Quad, largely because of the already effective alliance management it has imposed on its allies. The US has pushed Japan and Australia to participate in a joint effort against regional threats. Under its guidance, Japan became indirectly involved in the South China Sea, and Australia's presence in the Indian Ocean has become common. Even South Korea has publicly supported the US position in the South China Sea. To date, the US has strong leverage over its Asian allies who have accommodated its strategic interests by answering its calls. As the US already enjoys the high ground at the hub of its alliance

system, the Quad was only an inconspicuous element of cooperation between America's allies and non-allies and its importance quickly dropped after Washington had formally proposed FOIPS. The US showed more interest in deepening bilateral ties with Asian countries. As the US allies became stable supporters of its policies, the country had no reason to return to the Quad. Instead, the US dedicated itself to building security relations with strategic partners like Vietnam and India. The US encouraged its Asian allies to partner with each other and with its strategic partners, but either bilateral or multilateral, all cooperation was under its oversight.

At the same time, the members of the Quad may be hesitant to form a multilateral organization that targets China. India, for example, has tried to mend its relations with China since the 2017 Doklam standoff, an incident that was the most serious militarized confrontation since the Sino-Indian War. Modi paid a surprise visit to Xi a few months later to warm up bilateral ties (Haidar, 2018), and India remains cautious about partnering with the US allies. It declined Australia's request to join the annual Malabar exercise in 2018, and has been reluctant to portray the Quad as a quasi-security alliance (Grossman, 2019). Japan is another example. The country had advocated the Quad to enhance US–Japan–India and US–Japan–Australia trilateral ties (Tatsumi, 2018). It had particularly wanted to encourage India to get involved in the South China Sea (Jennings, 2017), but this enthusiasm dwindled after the US announced FOIPS. As the US showed less enthusiasm for the Quad, Japan lost interest in expanding it. It also failed to take a leading role in its revival.[17] Japan did not propose another meeting between the four states. Instead, it has focused on strengthening relations with the US, as discussed in the previous section.

Without the leadership of a great power, it is difficult to revitalize the Quad. The minor powers are also hesitant to further institutionalize the Quad. India fears being too antagonistic to China, while Japan and Australia are thus far unwilling to pay the costs of leadership, painting a grim picture for the organization's future. Even if Japan or Australia shows an interest in establishing a multilateral institution, the US is unlikely to show full support. The US does not need a multilateral institution to signal its resolve against Chinese expansion in the East China Sea, Taiwan Strait, or South China Sea when it can convey the same signal via bilateral alliances. Such signals can be even stronger through America's bilateral allies, as the US has been able to force its allies to mobilize resources. A multilateral institution would likely give minor powers more bargaining power over requests for US intervention in the region or make them

[17]In addition, India was not invited or consulted when Japan pushed the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). The CPTPP could have been the economic aspect of a multilateral effort led by Japan. Instead, the Quad was absent.

more resistant to contributing. The US does not want to lose its bargaining advantage, preferring to retain the ability to compel its allies to share security burdens in different parts of the Indo-Pacific. As the US has few reasons to organize multilateral cooperation, the current hub-and-spoke system is expected to strengthen and endure.

Conclusion: Tighter Alliances, Less Autonomy

The US and its allies in the Indo-Pacific have been aware of the rise of China and its impact on regional security. Since the Obama administration, the US has recognized the growing challenges in this region, mobilizing its Asian allies and partners in response. US allies have participated in defense cooperation with both the US and non-ally partners at its request. They have frequently engaged in military exercises, military assistance, and consultation with India, Vietnam, and the Philippines. The US has sailed with allies and partners in Northeast Asia, the South China Sea, and the Indian Ocean. Inter-alliance cooperation has increased significantly since 2016.

In light of the increased military cooperation, this paper examines whether multilateral defense cooperation, if not a treaty alliance, can emerge in the Indo-Pacific. The answer is that the US prefers the hub-and-spoke system to a multilateral mechanism. The chance of a more sophisticated multilateral security mechanism in Asia is low, and a NATO-like defense pact is highly unlikely. The argument rests on theories of alliance management and organization politics. The US enjoys a greater bargaining advantage in bilateral relations, and this advantage is particularly salient in Asia since the US is the main security provider. The current hub-and-spoke system in Asia helps the US manage its relationship with each ally, coordinating their defense policies to accommodate American foreign policy interests. President Trump's call for "America First" has caused the US to raise burden-sharing disputes with some allies and resulted in tense relations with them. Due to its significant influence on allies, the US has successfully pushed its Asian allies to invest in financial resources and military assets that accommodate its strategic interests. The allies cannot ignore the demands, nor can they join together to bargain with the US as unified whole. Since the hub-and-spoke system has helped the US fulfill its strategic interests, the US has little incentive to strengthen a multilateral consultation mechanism such as the Quadruple Security Dialogue even if it represents an opportunity to deepen its security partnership with India.

US allies have significantly increased their military relations with the country and with each other. They held joint military exercises, provided support with maritime

security, and coordinated their responses to China's claims in the South China Sea. This, however, does not suggest that they have more autonomy in their military relationships with other allies or non-ally partners. Instead, multilateral cooperation has been under the US supervision. The US has closely tracked joint cooperation between its allies and partners, making sure their cooperation accommodates its interests. For the past few years, US allies have not only faced growing pressure to adjust their bilateral security relations with the country, but also been encouraged to partner with third parties to build a presence in regional hotspots. Increased multilateral cooperation did not erode the hub-and-spoke system, but instead strengthened the US influence over its allies. The US, on the other hand, has strengthened its commitment to allies while directing them to improve military interoperability with strategic partners in the Indo-Pacific region. The US-led alliance system may appear to be a multilateral effort, but the allies have limited autonomy over their defense policies and alignment choices.

The strengthened hub-and-spoke system suggests that the security policies of US allies are constrained. They must accommodate US security interests as they build relations with China, North Korea, and other US strategic partners while showing firm support for the US position in the South China Sea dispute. Although none of the US allies or partners support China's claim in the South China Sea, countries such as South Korea used to be reluctant to get directly involved. As many scholarly works have pointed out, many Asian countries have adopted hedging policies to avoid being ensnared in the US–China competition. They have maintained various degrees of ambiguous positions between the US and China. However, US allies have found it more and more difficult to take a neutral position as the US has become more willing to confront China over both security and economic issues. This is particularly salient in the South China Sea dispute. Recently, South Korea and Australia have publicly pledged their support for the US position in the dispute. This shows that US allies are different from other non-ally partners. Due to alliance obligations and their dependency on US protection, US allies support the country's military strategy and political agenda in public even if they are sometimes reluctant to comply. The autonomy of allies has significantly decreased under the Trump administration, making it more difficult for US allies to carry out a hedging policy.

This does not imply that the autonomy of these allies will always remain so restrained. The current lack of policy autonomy is due to tense US–China relations and American security concerns in the Indo-Pacific. China's behavior in the South China Sea, the South Pacific, and the East China Sea is a key variable affecting the degree of policy autonomy among allies. If the trade dispute between China and the US can be

properly resolved or if China ceases provocations in disputed waters, the US would not require its allies to take as much action to defend their common interests. US allies would be able to pursue hedging policies that seek to maintain relations with both the US and China. On the other hand, the US would continue to enjoy dominance in each alliance dyad while still having no incentive to build a multilateral security institution in East Asia. There would still be no security network, let alone a security alliance. The US will continue to encourage and monitor defense cooperation between allies and partners, and it is expected to prevent any spontaneous efforts of alignment between its allies.

References

Abe, S. (2012, December 27). Asia's democratic security diamond. *Project Syndicate*. Retrieved from https://www.project-syndicate.org/onpoint/a-strategic-alliance-for-japan-and-india-by-shinzo-abe?language=english&barrier=accesspaylog.

Axelrod, T. (2018, October 19). Mattis: US, Japan, South Korea must work together against China on South China Sea. *The Hill*. Retrieved from https://thehill.com/policy/international/china/412190-mattis-us-japan-south-korea-must-work-together-against-china-on.

Bao, L. (2016, September 28). Japan's naval chief rules out joint-US freedom of navigation patrols. *Voice of America*. Retrieved from https://www.voanews.com/east-asia/japans-naval-chief-rules-out-joint-us-freedom-navigation-patrols.

Bennhold, K. (2019, March 19). German defense spending is falling even shorter. The U.S. isn't happy. *The New York Times*. Retrieved from https://www.nytimes.com/2019/03/19/world/europe/germany-nato-spending-target.html.

Benson, B. V., Bentley, P. R., & Ray, J. L. (2013). Ally provocateur: Why allies do not always behave. *Journal of Peace Research*, *50*(1), 47–58. doi: 10.1177/0022343312454445.

Burgess, S. F., & Beilstein, J. (2018). Multilateral defense cooperation in the Indo-Asia-Pacific region: Tentative steps toward a regional NATO? *Contemporary Security Policy*, *39*(2), 258–279. doi: 10.1080/13523260.2017.1386953.

Cha, V. D. (2016). *Powerplay: The origins of the American alliance system in Asia*. Princeton, NJ: Princeton University Press.

Chanlett-Avery, E., & Vaughn, B. (2008). *Emerging trends in the security architecture in Asia: Bilateral and multilateral ties among the United States, Japan, Australia, and India (CRS Report for Congress)*. Retrieved from https://fas.org/sgp/crs/row/RL34312.pdf.

Chipman, J. (2018, June 2). *Remarks by Secretary Mattis at Plenary Session of the 2018 Shangri-La Dialogue*. Retrieved from U.S. Department of Defense

website: https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1538599/remarks-by-secretary-mattis-at-plenary-session-of-the-2018-shangri-la-dialogue/.

Choe, S.-H. (2019, February 10). U.S. and South Korea sign deal on shared defense costs. *The New York Times*. Retrieved from https://www.nytimes.com/2019/02/10/world/asia/us-south-korea-military-costs.html.

Crescenzi, M. J. C., Kathman, J. D., Kleinberg, K. B., & Wood, R. M. (2012). Reliability, reputation, and alliance formation. *International Studies Quarterly*, *56*(2), 259–274. doi: 10.1111/j.1468-2478.2011.00711.

Emmott, R. (2019, November 7). Germany commits to NATO spending goal by 2031 for first time. *Reuters*. Retrieved from https://www.reuters.com/article/us-germany-nato/germany-commits-to-nato-spending-goal-by-2031-for-first-time-idUSKBN1XH1IK.

Gady, F.-S. (2019, August 1). Japan's marines storm beach alongside Australian, US troops. *The Diplomat*. Retrieved from https://thediplomat.com/2019/08/japans-marines-storm-beach-alongside-australian-us-troops/.

Gould, J. (2016, June 7). US names India 'major defense partner'. *Defense News*. Retrieved from https://www.defensenews.com/home/2016/06/07/us-names-india-major-defense-partner/.

Greene, A. (2019, June 23). Secret plans for new port outside Darwin to accommodate US Marines. *ABC News*. Retrieved from https://www.abc.net.au/news/2019-06-23/navy-port-us-darwin-glyde-point-gunn-marines-gunn-military/11222606.

Grossman, D. (2019, February 7). Quad supports US goal to preserve rules-based order. *The Strategist*. Retrieved from https://www.aspistrategist.org.au/quad-supports-us-goal-to-preserve-rules-based-order/.

Haftendorn, H., Keohane, R. O., & Wallander, C. A. (1999). *Imperfect unions: Security institutions over time and space*. New York, NY: Oxford University Press.

Haidar, S. (2018, April 14). Modi to fly to China soon to "reset" bilateral ties. *The Hindu*. Retrieved from https://www.thehindu.com/news/national/modi-to-fly-to-china-soon-to-reset-bilateral-ties/article23543175.ece.

Harris, A. H. B. (2016, March 2). *Raisina Dialogue Remarks — "Let's be Ambitious Together"*. Retrieved from https://www.pacom.mil/Media/Speeches-Testimony/Article/683842/raisina-dialogue-remarks-lets-be-ambitious-together/.

Hemmer, C. J., & Katzenstein, P. (2002). Why is there no NATO in Asia? Collective identity, regionalism, and the origins of multilateralism. *International Organization*, *56*(3), 575–607. doi: 10.1162/002081802760199890.

India-Australia joint naval exercises begin. (2019, April 3). *The Hindu*. Retrieved from https://www.thehindu.com/news/cities/Visakhapatnam/india-australia-joint-naval-exercises-begin/article26715538.ece.

Inoue, Y. (2010, September 29). China lifts rare earth export ban to Japan: Trader. *Reuters*. Retrieved from https://www.reuters.com/article/us-japan-china-export-idUSTRE68S0BT20100929.

Jacobs, J. (2019, June 25). Trump muses privately about ending postwar Japan defense pact. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2019-06-25/trump-muses-privately-about-ending-postwar-japan-defense-pact?fbclid=IwAR3Hl8TFR9d6za-qouGa2jNoK9WZxscoJACsIsPqSssWNDUYPyDWOb9Yq7wY.

Japan formally announces decision to buy F-35B stealth fighter jets from U.S. (2019, August 17). *The Japan Times Online*. Retrieved from https://www.japantimes.co.jp/news/2019/08/17/national/japan-formally-announces-decision-buy-f-35b-stealth-fighter-jets-u-s/#.Xuxt502P6Uk.

Japan supports but won't join US "freedom of navigation" patrols in South China Sea. (2017, February 6). *RT International*. Retrieved from https://www.rt.com/news/376410-japan-us-patrols-south-china/.

Jennings, R. (2017, September 20). India, Japan expected to increase maritime activity aimed at China. *Voice of America*. Retrieved from https://www.voanews.com/east-asia/india-japan-expected-increase-maritime-activity-aimed-china.

Jo, H. (2019, August 27). S. Korea faces prospect Trump may be seeking 'alliance fee'. *The Korea Herald*. Retrieved from http://www.koreaherald.com/view.php?ud=20190827000744.

Johnson, C. (2018, February 26). Australia caught in the middle of South China Sea conflict. *The New Daily*. Retrieved from https://thenewdaily.com.au/news/world/2018/02/26/south-china-sea-australia-usa/.

Johnson, J. (2019, May 9). Japan's Izumo helicopter carrier drills with U.S., India and Philippine militaries in disputed South China Sea. *The Japan Times Online*. Retrieved from https://www.japantimes.co.jp/news/2019/05/09/national/japan-izumo-drills/.

Joshi, S., & Graham, E. (2018, February 21). Joint freedom of navigation patrols in the South China Sea. *The Maritime Executive*. Retrieved from https://www.maritime-executive.com/editorials/joint-freedom-of-navigation-patrols-in-the-south-china-sea.

Jung, D. (2019, July 10). South Korea responds to US call for support on Indo-Pacific Strategy. *The Korea Times*. Retrieved from http://www.koreatimes.co.kr/www/nation/2019/07/356_272049.html.

Kahler, M. (1992). Multilateralism with small and large numbers. *International Organization*, *46*(3), 681–708. doi: 10.1017/S0020818300027867.

Kelly, T. (2018, September 27). Japanese carrier drills with British warship heading to contested South China Sea. *Reuters*. Retrieved from https://www.reuters.com/article/us-japan-defence-britain/japanese-carrier-drills-with-british-warship-heading-to-contested-south-china-sea-idUSKCN1M7003.

Kelly, T. (2019, August 30). Japan's military seek eighth straight annual hike in defense spending. *Reuters*. Retrieved from https://www.reuters.com/article/us-japan-defence-budget/japans-military-seek-eighth-straight-annual-hike-in-defense-spending-idUSKCN1VK0D2.

Kim, T. (2011). Why alliances entangle but seldom entrap states. *Security Studies*, *20*(3), 350–377. doi: 10.1080/09636412.2011.599201.

Kinne, B. J. (2018). Defense cooperation agreements and the emergence of a global security network. *International Organization*, *72*(4), 799–837. doi: 10.1017/S002081831800 0218.

Kitschbaum, E. (2019, August 9). U.S. envoy warns Germany: Pay more or risk losing protection. *Los Angeles Times*. Retrieved from https://www.latimes.com/world-nation/story/2019-08-09/us-envoy-warns-germany-pay-more-or-risk-losing-protection.

Krasner, S. D. (Ed.). (1983). *International regimes*, Cornell Studies in Political Economy. Ithaca, NY: Cornell University Press.

Lake, D. (1996). Anarchy, hierarchy, and the variety of international relations. *International Organization*, *50*(1), 1–33.

Lee, J. (2019, July 7). South Korea's US-China dilemma deepens with support for Indo-Pacific plan. *South China Morning Post*. Retrieved from https://www.scmp.com/news/china/diplomacy/article/3017509/south-koreas-us-china-dilemma-deepens-support-americas-indo.

Lee-Brown, T. (2018). Asia's security triangles: Maritime minilateralism in the Indo-Pacific. *East Asia*, *35*(2), 163–176. doi: 10.1007/s12140-018-9290-9.

Leeds, B. A. (2003). Do alliances deter aggression? The influence of military alliances on the initiation of militarized interstate disputes. *American Journal of Political Science*, *47*(3), 427–439.

Leeds, B. A., & Mattes, M. (2007). Alliance politics during the Cold War: Aberration, new world order, or continuation of history? *Conflict Management and Peace Science*, *24*(3), 183–199. doi: 10.1080/07388940701473054.

Leeds, B. A., Ritter, J. M., Mitchell, S. M., & Long, A. G. (2002). Alliance Treaty Obligations and Provisions, 1815–1944. *International Interactions*, *28*(3), 237–260.

Lieberthal, K. (2011, December 21). The American pivot to Asia. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2011/12/21/the-american-pivot-to-asia/.

Liu, R. (2018). Act East in the Indo-Pacific: India and Quad 2.0. *Prospect Journal*, *19*, 53–71.

Macias, A. (2018, October 11). "Why aren't they paying?": Trump hits out at South Korea about missile defense system. *CNBC*. Retrieved from https://www.cnbc.com/2018/10/11/trump-criticizes-south-korea-for-not-paying-for-missile-defense-system.html.

Macron, E. (2019, March 4). Emmanuel Macron: Dear Europe, Brexit is a lesson for all of us: It's time for renewal. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2019/mar/04/europe-brexit-uk.

Manyin, M. E., Daggett, S., Dolven, B., Lawrence, S. V., Martin, M. F., O'Rourke, R., & Vaughn, B. (2012). *Pivot to the Pacific? The Obama administration's "rebalancing" toward Asia* (CRS Report for Congress No. R42448). Retrieved from Library of Congress Washington DC Congressional Research Service website: https://apps.dtic.mil/docs/citations/ADA584466.

Martin, L. L. (1992). Interests, power, and multilateralism. *International Organization*, *46*(4), 765–792. doi: 10.1017/S0020818300033245.

Martin, L. (2019, May 29). Australian navy pilots hit with lasers during South China Sea military exercise. *The Guardian*. Retrieved from https://www.theguardian.com/australia-news/2019/may/29/australian-navy-pilots-hit-with-lasers-during-south-china-sea-military-exercise.

Mattes, M. (2012). Reputation, symmetry, and alliance design. *International Organization*, *66*(4), 679–707. doi: 10.1017/S002081831200029X.

Mehta, A. (2018, December 18). With massive F-35 increase, Japan is now biggest international buyer. *Defense News*. Retrieved from https://www.defensenews.com/global/asia-pacific/2018/12/18/with-massive-f-35-increase-japan-is-now-biggest-international-buyer/.

Mehta, A., Insinna, V., & Yeo, M. (2019, July 30). Japan wants to be an official F-35 partner. The Pentagon plans to say no. *Defense News*. Retrieved from https://www.defensenews.com/global/asia-pacific/2019/07/29/japan-wants-to-be-an-official-f-35-partner-the-pentagon-plans-to-say-no/.

Ministry of Defence, India. (2019a, April 2). *Third Edition of Bilateral Maritime Exercise Between Royal Australian and Indian Navies — AUSINDEX-19 set to begin*. Retrieved from https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1569974.

Ministry of Defence, India. (2019b, April 16). *AUSINDEX-19 concludes*. Retrieved from https://pib.gov.in/Pressreleaseshare.aspx?PRID=1570731.

Morrow, J. D. (1991). Alliances and asymmetry: An alternative to the capability aggregation model of alliances. *American Journal of Political Science*, *35*(4), 904–933. doi: 10.2307/2111499.

Morrow, J. D. (1994a). Alliances, credibility, and peacetime costs. *Journal of Conflict Resolution*, *38*(2), 270–297.

Morrow, J. D. (1994b). Modeling the forms of international cooperation: Distribution versus information. *International Organization*, *48*(3), 387–423.

Morrow, J. D. (2016). When do defensive alliances provoke rather than deter? *The Journal of Politics*, *79*(1), 341–345. doi: 10.1086/686973.

Narang, N., & LeVeck, B. L. (2019). International reputation and alliance portfolios: How unreliability affects the structure and composition of alliance treaties. *Journal of Peace Research*, *56*(3), 379–394. doi: 10.1177/0022343318808844.

Nguyen, M., & Pham, M. (2017, January 16). Japan pledges boats to Vietnam as China dispute simmers. *Reuters*. Retrieved from https://www.reuters.com/article/us-vietnam-japan/japan-pledges-boats-to-vietnam-as-china-dispute-simmers-idUSKBN15015O.

Noack, R., & McAuley, J. (2018, November 13). Why Trump's explosive claim that Macron wants a European military "to protect itself from the U.S." is so misleading. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/2018/11/10/why-trumps-explosive-claim-that-macron-wants-european-military-protect-itself-us-is-so-misleading/.

North Atlantic Treaty Organization (NATO). (2019, June 25). *Defence Expenditure of NATO Countries (2012–2019)*. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/20190625_PR2019-069-EN.pdf.

Olson, M. (1971). *The logic of collective action: Public goods and the theory of groups* (Rev. ed.). Cambridge, MA: Harvard University Press.

Olson, M., & Zeckhauser, R. (1966). An economic theory of alliances. *The Review of Economics and Statistics*, *48*(3), 266–279. doi: 10.2307/1927082.

Oye, K. A. (1985). Explaining cooperation under anarchy: Hypotheses and strategies. *World Politics*, *38*(1), 1–24. doi: 10.2307/2010349.

Page, J., & Jeong, A. (2018, September 28). South Korean warship sails by disputed South China Sea Islands. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/south-korean-warship-sails-by-disputed-south-china-sea-islands-1538127139.

Panda, A. (2019, July 7). South Korea and the US Indo-Pacific Strategy: At an arm's length? *The Diplomat*. Retrieved from https://thediplomat.com/2019/07/south-korea-and-the-us-indo-pacific-strategy-at-an-arms-length/.

S. Korea, Japan take part in U.S.-led Pacific naval exercise. (2019, May 23). *Yonhap News Agency*. Retrieved from https://en.yna.co.kr/view/AEN20190523006900325?section=search.

S. Korea rejects U.S.' renewed demand over cost sharing for strategic assets: Official. (2018, June 28). *Yonhap News Agency*. Retrieved from https://en.yna.co.kr/view/AEN20180628005800315.

Sandler, T., & Hartley, K. (2001). Economics of alliances: The lessons for collective action. *Journal of Economic Literature*, *39*(3), 869–896.

Schreer, B. (2016, February 25). The 2016 Defence White Paper, China and East Asia: The end of an illusion. *The Strategist*. Retrieved from https://www.aspistrategist.org.au/the-2016-defence-white-paper-china-and-east-asia-the-end-of-an-illusion/.

Singh, B. (2018, November 13). The Quad as an enabler of regional security cooperation. *The Strategist*. Retrieved from https://www.aspistrategist.org.au/the-quad-as-an-enabler-of-regional-security-cooperation/.

Smith, J. (2018, July 26). The return of the Indo-Pacific Quad. *The National Interest*. Retrieved from https://nationalinterest.org/feature/return-indo-pacific-quad-26891.

Snidal, D. (1985). The limits of hegemonic stability theory. *International Organization*, *39*(4), 579–614. doi: 10.1017/S002081830002703X.

Snyder, G. (1997). *Alliance politics*. Ithaca, NY: Cornell University Press.

Tatsumi, Y. (2018). *Is Japan ready for the Quad? Opportunities and challenges for Tokyo in a changing Indo-Pacific*. Retrieved from https://warontherocks.com/2018/01/japan-ready-quad-opportunities-challenges-tokyo-changing-indo-pacific/.

Tillerson, R. (2017, October 18). *Defining Our Relationship with India for the Next Century: An Address by U.S. Secretary of State Rex Tillerson*. Retrieved from the Center for Strategic & International Studies website: https://www.csis.org/analysis/defining-our-relationship-india-next-century-address-us-secretary-state-rex-tillerson.

Tow, W. T., & Stuart, D. (Eds.). (2014). *The new US strategy towards Asia: Adapting to the American Pivot*. Abingdon, UK: Routledge.

The U.S. Navy. (2019, June 18). *Wasp, Japan Maritime Self Defense Force ships sail in Philippine Sea*. Retrieved from https://www.navy.mil/submit/display.asp?story_id=109946.

The White House. (2017, May 25). *Remarks by President Trump at NATO unveiling of the Article 5 and Berlin Wall Memorials — Brussels, Belgium*. Retrieved from https://www.whitehouse.gov/briefings-statements/remarks-president-trump-nato-unveiling-article-5-berlin-wall-memorials-brussels-belgium/.

Verdier, D. (2008). Multilateralism, bilateralism, and exclusion in the nuclear proliferation regime. *International Organization*, *62*(3), 439–476. doi: 10.1017/S0020818308080156.

Walt, S. M. (1987). *The origins of alliances*. Ithaca, NY: Cornell University Press.

Waltz, K. N. (1979). *Theory of international politics*. Reading, MA: Addison-Wesley.

Weitsman, P. A. (2004). *Dangerous alliances: Proponents of peace, weapons of war*. Palo Alto, CA: Stanford University Press.

Wen, P., & Paul, S. (2018, April 20). China says had "professional" encounter with Australian warships in South China Sea. *Reuters*. Retrieved from https://www.reuters.com/article/us-southchinasea-australia/china-says-had-professional-encounter-with-australian-warships-in-south-china-sea-idUSKBN1HR035.

Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs
Vol. 56, No. 3 (September 2020) 2040010 (25 pages)

DOI: 10.1142/S101325112040010X

Interpreting Indonesia's "Look East" Policy: The Security Dimension of Foreign Aid

Baiq Wardhani and Vinsensio Dugis

As Indonesia's economy gradually improves, the government has been actively promoting its horizontal cooperation among developing countries by playing a prominent role as a non-DAC (Development Assistance Committee) provider. Though the country has been receiving aid over the past two decades, it has also been providing to other developing countries in the Pacific region. However, Indonesia's relations with these countries face contention due to it being perceived as "big and aggressive." This is evident in its decision to oppose the independence of Papua. After decades of seeking good relations, Jakarta has opened its Eastern door by creating a closer link with the Pacific countries through the provision of aid. As it moved from ignorance to awareness, Indonesia's approach was aimed at solving domestic problems related to its national integration and territorial integrity in the east, particularly the issue of Papuan independence. The country made use of aid as its primary diplomatic tool in its "Look East" policy. This paper investigates the extent to which this policy has been instrumental in rebuilding, restoring, and improving Indonesia's image among Pacific countries. It argues that the ethnic dimension is one of the critical determinants in diplomatic relations, and ignorance could lead to its failure. Furthermore, it shows that the use of aid has resulted in a constructive impact that has been evident in a decrease in support for Papua separatism in the South Pacific region.

Keywords: Diplomacy; identity; Pacific countries; Papua separatism; new donor.

* * *

Baiq Wardhani is a Lecturer at the Department of International Relations at Airlangga University, Surabaya, Indonesia. Her research interests include ethnicity, human security, foreign policy, and Pacific studies. She can be reached at <baiq.wardhani@fisip.unair.ac.id>.

Vinsensio Dugis is a Senior Lecturer at the Department of International Relations at Airlangga University, Surabaya, Indonesia. His research interests include foreign policy analysis, conflict resolution, border studies, and globalization and strategy. He can be reached at <vinsensio.dugis@fisip.unair.ac.id>.

This paper seeks to explain Indonesia's development assistance to the South Pacific in the realm of security by looking at development aid as a tool of securing its sovereignty in the issue of Papuan independence. Indonesia's development assistance to the Pacific is a part of the implementation of its foreign policy, which has two main aspects: to achieve national interests and to contribute to solving global problems (Ministry of Foreign Affairs of Republic of Indonesia, 2015a). Foreign aid is a critical means of addressing income disparity and poverty. Furthermore, the cosmopolitan view of foreign aid (Bayram, 2017; Kilby, 1999; Ulaş, 2016) implies a moral obligation: aid giving should do more good than harm to the recipient. At the same time, foreign aid has a "Janus-face" aspect which raises tensions between security interests and development assistance (Wasserman, 1983). Ideology, identity, and security factors inevitably influence the donor's attitudes since most donors act pragmatically according to their self-interest.

For almost two decades, Indonesia has been using various diplomatic tools to attract the people of countries in the South Pacific. These efforts do not appear to have been entirely successful since some countries continue to accuse Jakarta of serious human rights violations against indigenous Papuans. As a consequence, there have been repeated calls for the independence of Papua in various international forums (Wangge, 2016). One recent example was on January 26, 2019, when Benny Wenda, the exiled leader of the United Liberation Movement for West Papua (ULMWP), delivered a petition to UN Human Rights Chief Michelle Bachelet that was claimed to have been signed by 1.8 million Papuans and demanded a forum on Papuan independence. Wenda was able to attend the UN meeting with the help and support of officials from Vanuatu (Lin, 2019). Another example was at the 2016 UN General Assembly where Pacific island leaders used their speech time to publicly criticize Indonesia's rule in West Papua. In early March 2017, similar accusations were read by seven Pacific island nations during a session of the UN Human Rights Council in Geneva ("Pacific Nations," 2017).

Indonesia's poor image among several countries in the Pacific region can be explained by a combination of several factors. First, the country has displayed a strong Southeast Asian identity and had long ignored the Pacific region since the establishment of the Association of Southeast Asian Nations (ASEAN) in 1967 (Dugis et al., 2001). Second, although its gravest threats come from the region, the political adventures of several of the countries' former leaders have also added to its poor image. Indonesia has tried to address these problems through the use of developmental aid to gain sympathy from the Pacific region. These attempts have improved over the last decade, and the introduction of its "Look East" foreign policy has been one of the

several approaches to reverse its longstanding negative image among its neglected neighbors in the east. Therefore, this paper intends to investigate and analyze the extent to which this policy has been instrumental in rebuilding, restoring, and improving Indonesia's image among the Pacific countries. It also evaluates the effectiveness of aid as a significant component of a policy to improve the country's image in the region. The first section of this paper begins geographically from the South Pacific region, which was regarded as Indonesia's "backyard" as Southeast Asia was called its "front yard" in the 1970s. This geopolitical orientation is a result of a concentric circle formula in the country's foreign policy that places Southeast Asia in the first layer and the South Pacific in the second based on their respective geographical locations. The second section describes the emergence of Indonesia as a donor country. The third section discusses the relationship between Indonesia and South Pacific countries through the use of developmental aid and its impact, followed by our conclusions.

A Neglected Backyard

Indonesia began to show an awareness of the importance of the South Pacific region in the early 1970s. The combination of the domestic consolidation of Suharto's government and the Cold War environment forced Jakarta to admit the importance of its surrounding regions. After "securing" Southeast Asia with the establishment of ASEAN in 1967, Indonesia started to pay attention to the South Pacific region because the peace and stability of the region were *sine qua non* for its economic development (Dugis et al., 2001, p. 15). This stance is stipulated in the Broad Guidelines of the State Policy (GBHN),[1] formalized by the People's Consultative Assembly (MPR) through Decree No. 4, 1973, and those approved by the MPR in 1978 and 1983 (Usman, 1994, pp. 187–188) influenced other ASEAN members to adopt this view. This was evident at the Third ASEAN Summit in Manila in 1978, where one of the declarations explicitly stated that the body would promote and develop cooperation with both industrialized and developing countries in the Pacific region because of their dynamic and potential (Hadipranowo, 1991, p. 56). Furthermore, ASEAN accepted Papua New Guinea (PNG) immediately after it gained independence as an observer three years earlier (Dugis et al., 2001, p. 16).

[1]As stated in the document, the region is officially called the Southwest Pacific.

However, what was stated in these documents had not been fully operational in their implementation. Though about 10% of the population of its Eastern provinces are Melanesians (East Nusa Tenggara, Maluku, North Maluku, West Papua, and Papua), Indonesia admitted this belatedly, creating a series of diplomatic hurdles with its closest Eastern neighbors. Instead of being partners, they have seen the country from a negative perspective with some smaller states even developing anti-Indonesian sentiments. Indonesia's attention to the Pacific has been highly unbalanced compared to that toward ASEAN, the country's foreign policy cornerstone. Furthermore, the Suharto regime saw no economic benefit for the country to cooperate with Pacific countries as they also grappled with various problems such as poverty, high mortality rates, political instability, rampant corruption, and environmental issues. Despite the potential threats of these problems, Indonesia's foreign policy paid them no attention. Its gravest threat, the issue of Papuan separatism, was also yet to be addressed.

Furthermore, a low level of diplomatic relations existed between Indonesia and the countries of the South Pacific region. Throughout the 1970s, Jakarta only opened direct diplomatic relations with PNG at the embassy level with Port Moresby being supported by the Consulate General of the Republic of Indonesia in Vanimo and one Consulate General of PNG in Jayapura, Indonesia. It also maintained diplomatic relations with Fiji, which started through the signing of a Memorandum of Understanding (MoU) in Wellington, New Zealand, by the Indonesian Ambassador to New Zealand and the Fijian High Commissioner for New Zealand in 1974. A similar relationship was opened with Vanuatu in 1980, with few other countries of the region being added until the 1990s when Jakarta started developing diplomatic posts.

Ethnic similarities with Melanesian societies in Indonesia's east have stimulated the continuing support for Papuan independence among Pacific countries. According to a senior Indonesian diplomat, most Pacific countries as newly independent nations failed to understand Indonesia's enormous ethnic diversity and their apprehension ought to be understood. Though the Pacific countries are also very diverse, they are also bound by many obstacles such as distance and remoteness. As the most significant part of the population in the region, Melanesians have a strong unity base that has been described as "Melanesian Brotherhood." Although this was originally a religious concept, it has been since politicized and used to support the secessionist movement in Papua, which is home to a Melanesian majority. Moreover, strong support from Vanuatu to the Free Papua Movement (OPM) has been one of the factors influencing the ethnically-based sympathy that has been used as moral capital for the continuation of their struggle. This support can be associated with the "ethnic nepotism" model, which takes place in international relations (Vanhanen, 1991). Ethnic identity is

another significant factor utilized by secessionists in achieving their objectives. While identity provides a space for separatist groups to express their differences with others, choosing the right identity is strategic in attracting international attention. Ethnic leaders maximize symbols, myths, traditions, and practices to reinforce their identity (Saideman, Dougherty, & Jenne, 2005).

The double identity of Indonesia, as a part of both Southeast Asia and the Pacific, became apparent at the end of the 1980s after many Pacific countries opposed the country's annexation of East Timor in various international fora, including the UN. This move almost resulted in a total failure of diplomacy between the country and the region. To complicate the problem, the secessionist movement in Papua gathered strength after the independence of East Timor in 1999. Due to the mistreatment of East Timoreons combined with successful lobbying from Papuans in exile, Indonesia's image suffered greatly among the Pacific countries. Due to these unfavorable circumstances, the country intensified its diplomatic approach to the region through more visits and road shows, and these produced positive results. The provision of developmental aid was another effort of the country to strengthen cooperation with the region and a part of a larger plan to develop Papua and its Eastern provinces. Indonesia's attention to the region continued to increase during the 1980s. In 1983, the Indonesian Minister of Foreign Affairs at the time, Mochtar Kusumaatmadja, made a continuous visit to PNG, Fiji, Western Samoa, and the Solomon Islands to offer assistance through a scheme called Technical Cooperation between Developing Countries, receiving a positive response (Usman, 1994, p. 196). Undoubtedly, this was the beginning of Indonesia's more tangible engagement. According to Minister Mochtar, it was the right time for Indonesia to visit the region which has long been regarded as the second layer in the context of the country's foreign policy. Cooperation in the economic sector also began to increase since then, and a year after this visit, diplomatic relations with Western Samoa were officially opened (Dugis et al., 2001, pp. 18–20).

Meanwhile, several developments increased Jakarta's confidence in these diplomatic endeavors. First, Papua was perceived to be weak, and with a small "army," it would be technically easy for the Indonesian army to defeat it. Second, Papua is geographically isolated, making it relatively more difficult for external parties to support their struggle for independence. Third, the OPM is as of yet non-monolithic and tribal in essence, with many groupings based on linguistic and regional loyalties that limit its ability to campaign widely and effectively. These conditions convinced Jakarta that it would be difficult for OPM leaders to garner diplomatic support for the success of their cause. However, Pacific countries continuously questioned Indonesian

sovereignty in Papua, and strong moral and diplomatic support to the secessionist movement was evident at the end of the 1990s and peaked in 2000, especially after the independence of East Timor. Furthermore, the development of new international issues such as human rights violations and environmental destruction in Papua has drawn international attention. These issues became "new energy" for the Papuan independence movement and gained support among several Pacific countries.

Several crises marked the rise of support for the Papuan independence movement in 2000, especially after the separation of East Timor in 1999. The political situation at the end of the 1990s was very conducive for the revival of Papuan self-determination, an issue which was considered to be unfinished by countries in the Pacific region. The Second Papuan People's Congress in 2001[2] inspired many Papuans to pursue independence and had greatly hurt the image of the Indonesian Government, and the country needed to take strategic steps to repair it. This can be actualized by paying attention to cultural–psychological roles when conducting diplomatic relations, especially with countries in the Pacific region. The country should also be able to find the positive side of the Melanesian Brotherhood and make sure the concept brings no harmful effects. Security issues in Eastern Indonesia such as conflicts in Maluku and Poso[3] may hurt Indonesia's image and lead to difficulty in establishing diplomatic relations with the Pacific countries. Although Indonesia managed to establish relations with some of these countries, it must work harder to foster better relations with PNG and Vanuatu as PNG is a crucial player in the region. At the same time, Vanuatu is still sympathetic to the Papuan independence movement, and Jakarta is expected to formulate a more tactical and Pacific-oriented policy. Furthermore, although the OPM is militarily weak and its people are relatively less cohesive, the government is concerned about Papua gaining support through historical, religious, and ethnic factors which are weak points in Indonesian sovereignty. Therefore, a failure of Indonesian diplomacy in the Pacific could have a counterproductive effect on the government's efforts to maintain its territorial integrity.

As the Pacific countries themselves are beset with domestic and regional problems and perceive themselves as "weak," "failing," or "failed states" in the Melanesian sub-region (Reilly, 2004), they are also concerned with supporting their ethnic kin across borders. Threats to the region's stability can in turn threaten Indonesia's security. At the same time, it is in the country's interest to foster a better diplomatic relationship through regional intergovernmental organizations such as the Pacific

[2]According to the OPM leaders, the First Papuan People's Congress occurred in 1961.

[3]The conflicts in Maluku and Poso were the worst sectarian conflicts in the post-Suharto era, which took place between 1998 and 2001.

Islands Forum (PIF), Melanesian Spearhead Group (MSG), and Pacific Islands Development Forum (PIDF). To this end, Indonesia has regarded the region as second only to Palestine in its provision of developmental and technical assistance.

From Recipient to Donor

Foreign aid is all forms of goods and services owned and managed by the donor country, where the allocation varies depending on their goals and interests. This definition is similar to that proposed by the Development Assistance Committee (DAC) of the Organisation for Economic Co-operation and Development (OECD). Foreign aid includes the transfer of public resources from one country to another or to non-governmental organizations, where 25% of the components are granted elements that aim to improve developing countries. There are three kinds of foreign aid: as a form of resource allocation, as a form of giving, and as a form of symbolic dominance (Hattori, 2001, p. 634).

After more than 50 years of being both a donor and a recipient, Indonesia has also been playing a prominent role as a non-DAC provider. The country has been able to limitedly promote Technical Cooperation among Developing Countries (TCDC) through the Indonesian Technical Cooperation Programs (ITCP) since 1981. This achievement is part of a long historical development, as Indonesia was initially the initiator of South–South Cooperation (SSC) at the Asian–African Conference and the Non-Aligned Movement. The country's important role in the global coloring order is a manifestation of its role as an assertive global power at that time. Based on the Final Communiqué of the Asian–African Conference of Bandung, Third World countries agreed to work together to achieve development and economic growth through agreements over technical cooperation and the formation of horizontal relationships (Walz & Ramachandran, 2011, p. 10). In contrast to traditional vertical aid from Northern and Western countries, South–South Cooperation is a form of horizontal relations that allows countries to cooperate to solve common problems (Klingebiel, 2014, p. 19).

The emergence of new non-DAC providers has been explained by Walz and Ramachandran (2011), Marx and Soares (2013), Trinidad (2014), Klingebiel (2014), and Carle (2015). They have generally examined a trend in which many developing countries have gained the confidence to scale up their status and become new aid givers. In order to explain this, Trinidad (2014, pp. 76–77) proposed a theory of four stages of recipient-to-donor donations based on the transformation of the three

developing countries of Indonesia, Thailand, and the Philippines that became new donors. Trinidad (2014) observed that these countries have undergone the stages of incubation, transition, emerging donor status, and becoming a major donor. The first period is characterized by the role of new-coming developing countries as they offer aid to fellow developing countries in technical cooperation while continuing their status as recipients of aid from DAC countries. The second period was marked by Indonesia's activity as an emerging donor promoting technical cooperation through South–South Cooperation, a more institutionalized forum which provided the opportunity to share experience, learn, and conduct networks with developed countries while enabling the elevation of its status to the third period. Due to its commitment as a donor, Indonesia's emerging status gained recognition from developed countries. This status has provided the country with greater confidence to fully implement its aid commitments. The final period is one in which a country becomes significant donor and its status has been elevated to that of other developed countries on the DAC. Indonesia's experience shows that it is still in the third stage, a transitional period that was marked by a change in status from a lower- to a middle-income country in 2008 and it becoming a member of the Group of 20 (G20) (Siliwanti, 2011). The country's transition from being a recipient to a non-traditional donor as a result of its growing economy marked its new identity in the global aid landscape. Apart from being a member of MINT (Mexico, Indonesia, Nigeria, and Turkey), Indonesia is aligned with the BRICS (Brazil, Russia, India, China, and South Africa), and more importantly, it is a member of the G20. According to these factors, the country is predicted to become one of the top 10 global economic players in the next decade (Martinez, 2016).

One significant milestone in Indonesia's transition was the signing of the Jakarta Commitment, an agreement between the government of Indonesia and 26 Development Partners on January 12, 2009. This document was a shared commitment of governments and development partners to enhance the effectiveness of external financing in Indonesia (Jakarta Commitment, 2009). It also means to uphold the vision of the country and its development partners to jointly strengthen the ownership of recipient countries in their development assistance and maximize the impact of aid. Moreover, the document stipulates the need to further improve the international governance of aid and the strengthening of South–South Cooperation. Indonesia's considerable success as an emerging middle-income country has been said to be an excellent example for other developing countries. Together with its development partners, the country has committed itself to further strengthening regional processes and institutions facilitating South–South Cooperation

(Jakarta Commitment, 2009, pp. 2–3). South–South and Triangular Cooperation (SSTC)[4] has become part of the country's foreign policy agenda (National Coordination Team of SSTC, 2015, p. 1) as according to the Director for the Technical Cooperation of the Ministry for Foreign Affairs (MOFA) of Indonesia, Siti Nugraha Maulidiah, Indonesia contributed approximately US$49.8 million between 2000 and 2013 (Maulidiah, 2013).

Indonesia maintains the image of a recipient-turned-donor country based on a combination of its achievements in the successful management of its foreign debt, its "prosper-thy-neighbor" policy, and its regional power strategy. As previously stated, the SSTC is the primary mechanism used by Jakarta in carrying out its roles in various programs of different ministries and agencies that include capital market development, water management, corruption eradication, and technical cooperation (The United Nations Development Programme [UNDP] 2015). In 2012, the country opted to prioritize three sectors which are development issues covering poverty alleviation, disaster management, climate change, and human development; governance issues comprising of good governance and peace-building democracy as well as law enforcement and peacekeeping; and economic matters including macro-management, public finance, and micro-finance (The Asia Foundation, 2014). Overall, Indonesia has four objectives in carrying out its role as a donor. These include maintaining traditional solidarity, contributing to national diplomacy, creating business opportunities, and supporting transitions to democracy. While the first objective is related to the country's long traditional relations with developing countries, the second relates to "countries that are important to Indonesia's diplomacy, and particularly where it encounters political challenges such as the South Pacific (Melanesian Spearhead Group - MSG) countries, which have been declared a priority for SSC" (UNDP, 2015). Meanwhile, the two other objectives are the newest and are sometimes seen as an investment for future broader relations.

The momentum of Indonesia's emergence as a non-DAC provider coincided with an overall global trend of decreasing aid to developing countries. According to the OECD, it declined by 2.4% in 2011 with least developed countries receiving the greatest impact (OECD Library, 2014, pp. 98–99). The situation was even worse for the South Pacific countries, where foreign development aid served as the primary

[4]The UN defines South–South Cooperation as "a process whereby two or more developing countries pursue their individual and/or shared national capacity development objectives through exchanges of knowledge, skills, resources and technical know-how, and through regional and inter-regional collective actions ...." Meanwhile, SSTC is South–South Cooperation supported by a Northern partner (International Labour Organization, n.d.).

source of revenue (Gani, 2006). Therefore, one of their major issues was to overcome aid dependency from traditional donors, especially their colonial powers. More than 50% of aid for Pacific countries comes from Australia as "the big brother" to the Pacific (Pryke, 2013). Australia provided AU$6.8 billion in bilateral aid to the region between 2006 and 2013, while Canberra has reduced its aid by 10% to overall Pacific countries, including regional organizations (Hayward-Jones, 2015). During this period of aid shortage from traditional donors, Indonesia increased the amount of its aid through various endeavors in the Pacific.

Furthermore, the architecture of foreign aid changed with the inclusion of new players, dubbed as emerging donors. As the Cold War eased, the nature and pattern of foreign policy and aid gradually shifted. As Hopkins (2000) puts it, "foreign policy is more geared towards international public goods, including containing international 'bads'." New players in foreign aid emerged and played essential roles in contributing to the development of recipient countries. Indonesia made use of this opportunity by aiding neighboring Eastern countries through increments in national security, including traditional and non-traditional security issues under the principle of "prosper thy neighbor." As regional stability is vital to the security of any country, an event of instability has a direct effect on the stability of donor countries (Walz & Ramachandran, 2011). Indonesia has realized that its "backyard" is inhabited by several countries suffering from severe economic hardship, and this could be a direct threat to its territorial integrity. Therefore, its foreign policy was directed toward "the structural power pattern in the global system" (Picard, Groelsema, & Buss, 2008, p. 14). As revealed earlier, the country prioritized the South Pacific countries in its SSTC, particularly for its second objective of contributing to national diplomacy (UNDP, 2015).

Opening the Eastern Door

The decreasing level of financial assistance from traditional donor countries to the South Pacific region paved the way for other donors such as China, Taiwan, and India (Wardhani, 2015). As the countries of the region faced common financial problems, they also declared a need for external support for Papuan independence. Indonesia in turn strengthened its "Look East" policy to further open its Eastern door by intensifying developmental assistance. The provision of aid to Pacific countries is instrumental to Indonesia's interest in keeping the region under its control in order to ensure that any agitation there does not harm its position, particularly concerning its

sovereignty over Papua. Jakarta increased its presence using development as a diplomatic instrument with the hope that it would "win the hearts of the people," and this resulted in the decline of external support for the Papua separatist movement in the countries of the region. This strategy was implemented in spite of the fact that the region does not offer any economic benefits to Indonesia due to its limited markets and troublesome domestic politics.

Indonesia's aid to South Pacific countries aims at the following:

(a) To secure Indonesia's territorial integrity, particularly in regard to issues of Papuan separatism. This reason is first and foremost for any Indonesian aid to the region. Whereas the governments of many Western countries and aid organizations have revised their aid strategies in response to new security concerns in the conflict-prone countries, Indonesia does not follow this "securitization" trend. The country defines its security primarily around the concept of its "concentric circles."[5]
(b) Extending Indonesia's role as a new donor country, as Indonesia believes it has good justification for its foreign policy toward the Pacific countries, and the South Pacific is the second priority of its foreign policy.
(c) To materialize and strengthen its commitment to South–South Triangular Cooperation. Although the amount of assistance is comparatively insignificant to the amount that has been offered by traditional donors, Indonesian aid is a form of "solidarity" and its SSTC commitments represent the ideal use of foreign aid. There is awareness among Pacific countries that this development assistance is primarily intended to bolster friendship and mutual cooperation, and though it is a fellow developing state, Indonesia intends to shoulder the entirety of the burden. South Pacific countries also see Indonesia as an alternative to the strategic diversification of their diplomatic relations, as it is their most prominent neighbor to the south.

In essence, Indonesia's "Look East" policy prioritizes South Pacific countries as partners in cooperation for development using various bilateral, trilateral, and multilateral mechanisms through other regional organizations (Tahalele, 2016). Since 1999, the country has delivered over 90 capacity-building programs to more than

[5]"Concentric circles" is a concept that describes Indonesia's foreign policy priority based on geographic proximity. This concept gained currency when Mochtar Kusumaatmadja served as the Indonesian foreign minister from 1978 to 1988 and continued to be popular until the end of the New Order.

500 Pacific Islanders (SSC-Indonesia, 2015). Between 1999 and 2009, it extended its development assistance through training in nine different sectors of marine and fisheries; SMEs, economy, finance, and trade; energy, democracy and good governance; media and ICT (Information and Communication Technologies); agriculture and forestry; disaster risk management; public works; education, culture, and diplomatic training; and health. The program attracted many participants and was continued for the next five years from 2010 to 2014 and modified to include 10 sectors of marine and fisheries, energy, media and IT, agriculture, democracy and good governance, disaster risk management, tourism, women's empowerment, education, culture, and diplomatic training, and public works (SSC-Indonesia, 2015).

Attention and aid to Pacific countries were intensified during the administrations of Presidents Abdurrahman Wahid and Megawati Sukarnoputri, with some indication that the initiative succeeded. In December 2000, Megawati in her capacity as Vice President made a two-day visit at the invitation of the Prime Minister of PNG to celebrate 25 years of its independence. Indonesian Ambassador to PNG Benny Mandalika said on the occasion that Megawati had the opportunity to inaugurate a statue of her late father, Indonesia's first president Sukarno, in the capital city of Port Moresby. According to the Chairman of the National Celebration Council of PNG Peter Barter, this visit was an honor for the country (Radio Australia, 2000). Vice President Megawati held a meeting with Governor General Silas Atopare and Prime Minister Mikere Morauta on bilateral borders, security issues, and trade relations during the visit. Megawati acknowledged that trade relations were discussed because the South Pacific region was still not getting enough attention from Indonesia, and an MoU was signed between the Minister of Industry and Trade, Luhut Binsar Pandjaitan, and the Deputy Minister of PNG Foreign Affairs, Moi Avei. Following the visit, Megawati revealed that PNG had offered its full support for Indonesia's territory, especially by recognizing Papua as part of the Unitary State of the Republic of Indonesia/NKRI (Kompas, 2000).

One indicator showing Indonesia's presence in the South Pacific was its official acceptance as a Pacific Islands Forum Dialogue Partner in 2001. Its acceptance was delivered by the chairman of the forum, Kiribati President Teburo Tito, through a letter sent to President Wahid in mid-April 2001. The letter was in response to a request made by the country in October 2000 during the 31st PIF Summit in Tawara, Kiribati, where member states agreed to change the name of the organization from the South Pacific Forum (SPF) to the Pacific Islands Forum. The aim was to expand the scope of cooperation by involving not only states in the South Pacific region but also others in nearby regions (Deplu RI, n.d.).

The Indonesian Government stepped up its development assistance to South Pacific countries following its inclusion in the PIF. There was an intensification of aid programs conducted since 1999 such that between 1999 and 2016, the country had run at least 182 programs for 1,457 participants from countries in the Pacific region under the framework of South–South Cooperation. According to the Director of Technical Cooperation for the Foreign Ministry of Indonesia, Syarif Alatas, technical assistance was based on equality, solidarity, demand, mutual respect, mutual benefit, and unconditionality. The technical assistance provided included fisheries, agriculture, democracy and good governance, disaster risk management, seaweed processing techniques and entrepreneurship, forestry, health, education, climate change, community empowerment and women's development, SME, trade, finance, industry, public order management, information and communication technology, infrastructure, energy and mineral resources, tourism, and arts and culture. Having recently established trade ties with Indonesia and other Pacific countries, Samoa received increased technical assistance and capacity-building programs in the form of bilateral and triangular cooperation agreements (Radio New Zealand, 2017). However, Indonesia still needs to expand the forms and quantity of its assistance to Pacific countries to strengthen its relationship with its Eastern neighbors, and more importantly, to maintain the sustainability of these endeavors.

Indonesia's inclusion into the PIF is politically strategic, especially concerning the issue of separatism in Papua. This step has provided Jakarta an excellent opportunity to have firsthand information about the position of countries in the South Pacific on the issue and also to provide balanced information on what has been done in order to address it (Dugis et al., 2001, p. 25). Positive results were seen shortly afterward, and at the end of the 2001 PIF Summit, the members agreed in a final communiqué that Indonesia was a sovereign party to Papua (FORUM Communique, 2001). The South Pacific Forum recognized Indonesia's sovereignty over the territory of Papua, which they explicitly referred to as an Indonesian province. They also acknowledged that a "special autonomy" policy for Papua would be the ultimate answer to the several violent issues occurring in the country. Therefore, the PIF countries made no official mention of any support for the separatist movement in Papua (Kompas, 2001a). In response, the Indonesian Government offered to increase diplomatic relations with several countries in the region, beginning with direct diplomatic relations with Fiji where the Secretariat of the Pacific Islands Forum is located (Kompas, 2001b). In the practical relations between Indonesia and these countries, this decision has allowed for much improvement compared to the previous decade and was evident in the increase of diplomatic, economic-trade, and socio-cultural relations.

This policy was extended during the term of President Susilo Bambang Yudhoyono through PIDF[6] as a triangular partnership involving the public sector, private sector, and civil society to "tackle the complex sustainable development challenges" faced by the region (Pacific Islands Development Forum, 2015). Assistance to these countries was materialized through a green economy scheme. The low-lying island nations were facing the grave threat of climate change to the extent that Kiribati, Tuvalu, and Marshall Islands were about to go into extinction. Indonesia channeled this aid through the South–South Cooperation, which was well suited to the PIDF's needs.

To express the country's commitment, President Yudhoyono gave a presentation at the 2nd Pacific High-Level Development Forum on June 19, 2014. The President as the first to visit Fiji reiterated that the visit was ". . . in line with my commitment for the past decade to deepen and strengthen relations with this important region" (Pacific Islands Development Forum, 2014). Indonesia restated its commitment to assist in the development of the green economy, a new paradigm that drives economic progress without harming natural resources and copes with the impact of climate change (Pacific Islands Development Forum, 2014). This is a strategic move by the country because the main threat for Pacific countries is not military but environmental (Shibuya, 2003, pp. 137–138). For tiny island states such as Tuvalu, Kiribati, and the Marshall Islands, it is a genuine and immediate existential threat (Wyeth, 2017).

Indonesia also strengthened its relations with Fiji, which is the founder of the PIDF. An interviewee from the Indonesian MOFA remarked that Fiji is a vital and longstanding partner of Indonesia, and thus, the country is confident that Fiji would help it win sympathy from other Pacific island countries. According to the Australian-based radio station ABC, President Yudhoyono expressed his hope that Indonesia would work closer with Fiji since the country can serve as the "engine of Pacific Island countries' growth." Fiji is the best partner in the region to act as a strategic communicator for the interests of Indonesia. In order to promote peace in the country, Jakarta pledged to support Fiji and the PIDF by tripling the amount of its aid to US$1 billion in the coming years. More importantly, with the support of Fiji and PNG, Vanuatu dropped its boycott on Indonesia during the MSG Meeting in 2014 and made sure that the United Liberation Movement for West Papua (renewed OPM) would not

[6]The PIDF is "a space for catalyzing, mobilizing and mainstreaming action in support of sustainable development through a green economy in Pacific Island Countries." The members of this regional forum are American Samoa, the Commonwealth of the Northern Mariana Islands, the Cook Islands, the Federated States of Micronesia, Fiji, French Polynesia, Guam, Kiribati, the Marshall Islands, Nauru, New Caledonia, the Pitcairn Islands, Samoa, the Solomon Islands, Timor-Leste, Tonga, Tokelau, Tuvalu, Vanuatu, Wallis, and Futuna (see <http://pacificidf.org/what-is-pidf/>).

meet anyone without the approval of Indonesian authorities (Radio ABC, 2014). This decision was a diplomatic triumph for Indonesia since the MSG was a source of support for the efforts of Papuan independence activists.

It is noteworthy that despite its political–diplomatic objectives, Indonesia's aid to South Pacific countries also served as a form of commitment to strengthen the co-operation needed to mitigate climate change issues (Kementerian Luar Negeri, 2014). This assertion was conveyed through the Palau Declaration of the 26th Meeting of the Pacific Islands Forum Post-Forum Dialogue (PIF-PFD) with the consideration of the maritime characteristics of Indonesia. The Declaration stressed the importance of addressing global warming and rising sea levels, and Indonesia also provided US$1 million in aid to Palau for the 45th Pacific Islands Forum Meeting held from July 29 to August 1, 2014 (Kementerian Luar Negeri, 2014). The country's "Green Economy" strategy was therefore well received by the Pacific countries because it suits their interests.

President Joko Widodo has continued Indonesia's open-door policy toward its Eastern neighbors by strengthening its commitment after the 2nd PIDF Summit. This commitment was evident when the country sent a scoping mission team to PNG and the Solomon Islands during June 8–17, 2015 as a follow up to President Yudhoyono's visit in 2014 and a meeting with the Foreign Minister to PNG on February 27, 2015 at Port Moresby (KBRI Port Moresby and Kementerian Luar Negeri, 2015). The team was headed by Ambassador Andreas Sitepu (the former ambassador for PNG from 2010 to 2014), with its main agenda being devoted to capacity-building assistance to PNG and the Solomon Islands in accordance with their individual needs. The team also brought a craft machine and some experts to help the economic empowerment of environmental-based Small and Medium Enterprises (KBRI Port Moresby and Kementerian Luar Negeri, 2015). To remind its Pacific neighbors that a majority of Melanesians live in Indonesia, the government conducted the first Melanesian Cultural Festival in Kupang, East Nusa Tenggara from October 27 to October 30, 2015, and representatives from PNG, Fiji, New Caledonia, the Solomon Islands, Vanuatu, and Timor-Leste attended (Fardah, 2015; Putri, 2015). The festival was significant because it was the first since independence and represented the country's belief in showing a serious commitment to the welfare of Melanesians. As such, it has helped Indonesia pave the way for a diplomatic victory.

In 2016, President Joko Widodo sent another team led by the Coordinating Minister for Political, Legal, and Security Affairs, Luhut Binsar Pandjaitan, to Fiji and PNG to demonstrate Indonesia's commitment to bilateral relations. Minister Pandjaitan delivered 100 units of hand tractors to assist the development of

agriculture, US$3 million in financial aid, and US$3 million worth of goods to assist victims of the Tropical Cyclone that hit Fiji in late February 2016. Indonesia's diplomatic approach toward Papuan secessionism was strengthened through a proposal of Fijian Foreign Minister Ratu Inoke Kubuabola that the country should be promoted from an associate to a full member of the MSG. In addition to Fiji, the relationship with PNG was also reinforced through Prime Minister Peter O'Neill's invitation to President Joko Widodo to visit Port Moresby from May 11 to May 12, 2016 in order to strengthen bilateral cooperation in economic construction, trade, investment, and infrastructure. The two leaders also agreed to increase the value of bilateral trade outside of business activities to the tune of US$4.5 million per year (Fardah, 2016). Foreign Minister Retno Marsudi has asserted that Indonesia's new aid agency, called the Agency for International Development (AID), is the country's channel for the G20 economy to help other countries achieve sustainable development goals. Indonesia feels obliged to provide its Eastern neighbors with development aid and disaster relief to smaller countries by allocating an initial budget of about IDR 3 trillion (US$212 million). Vice President Jusuf Kalla claimed, "The main objective is to increase our diplomacy effort to help partnership with other developing countries to tackle issues like refugees or conflicts" ("Indonesia Creates," 2019). Even though the Vice President emphasized there was no link to Papua-related diplomacy, it is difficult to conclude that this aid is not a political tool for Indonesian diplomacy to win the "hearts and minds" of the people in these countries.

One further indication of Indonesia's presence in the South Pacific region is its eventual elevation as an associate member in the MSG in 2015 from the observer status it gained in 2013. This is a diplomatic success for several reasons. First is the fact that the MSG is the most potent political–economic alliance in the South Pacific region. The total population of the four member countries of the MSG (PNG, Vanuatu, the Solomon Islands, and Fiji) is three-quarters of the total population, land, and gross domestic product (GDP) of all 14 countries in the region (Pacific Institute of Public Policy, 2008). The 10 other countries of the region in MSG are Nauru, Kiribati, the Marshall Islands, the Micronesian Federation, Palau, Tonga, Samoa, Tuvalu, Niue, and the Cook Islands. While Indonesia's inclusion in the MSG had already indicated its bold presence in the region, being an associate member further strengthened this position (Andhika, 2015).

The second is related to the issue of Papuan separatism. Since the formation of the MSG, separatists have had an avenue to voice their struggle, and because of the Melanesian cultural equation, a certain section of independence supporters wanted the struggle to be the organization's main agenda (Lawson, 2016). This is the reason why

the Indonesian Government has focused its attention on the group from its inception. In a statement at Halim Perdana Kusuma Airport, Jakarta, shortly before flying to Fiji in 2014, President Yudhoyono said that since many organizations have provided a platform for political campaigns for Papua separation, there is a need to establish a healthy and good relationship with countries in the South Pacific (Waluyo, 2014). The President stated that the MSG and other organizations have been "often used as an avenue to support the Free Papua Movement" and "want to attract blocks in the face of Indonesia." Therefore, it is his job "to increase the friendship and cooperation with those countries and explain our true policy on Papua" so that "the misinformation on the Papua issue and what Indonesia is doing can be eliminated" (Waluyo, 2014). This statement indicates that the direct involvement of Indonesia in MSG activities is both essential and strategic. Therefore, the country provides direct information on conditions in Papua to countries in the South Pacific region and gives its representatives the opportunity to see them personally. This offer was evident in President Yudhoyono's statement that he was pleased with the visit by the delegations of MSG foreign ministers and permitted them "to visit Papua and other places in Indonesia to hear firsthand information and look directly at the situation of Papua as well as our policy with regards to justice, economic development, and security in the area" (Waluyo, 2014).

In order to strengthen its political position, Indonesia also demonstrated the possibilities of broader economic cooperation opportunities for MSG member countries. Despite its membership status as an observer before 2015, the country has been able to contribute considerably to these countries. Since 2011, it has implemented 130 technical assistance programs attended by approximately 500 people (Ministry of Foreign Affairs of Republic of Indonesia, 2015b). In the economic context, it has also served as a "bridge" between the MSG and Asia in general by making it possible for member countries to benefit from the fastest-growing Asian economy. The Head of the Policy Analysis and Development Center of the Indonesian Ministry of Foreign Affairs, Siswo Pramono, argued that there are plenty of opportunities available in Asia through Asia-Pacific Economic Cooperation (APEC), the Trans-Pacific Partnership (TPP), the Regional Comprehensive Economic Partnership (RCEP), and the ASEAN Economic Community (AEC) (Pramono, 2016). It has been reported that "APEC, TPP, RCEP, and AEC represent the geopolitical shift towards East Asia." Therefore, the political reorientation of MSG members toward Asia through the "Look North Policy" is not only sensible but also *a sine qua non* (Pramono, 2016).

It is in this context that the elevation of Indonesia from an observer to associate status since 2015 has had strategic value. This new status makes it possible for the country to be involved more intensely and directly in various activities with MSG

Table 1.
Indonesia's Aid to the South Pacific Countries in 2019

No.	Sector	Amount
1	To improve the image of Papua	IDR 20 billion
2	To strengthen cooperation with South Pacific International Organizations	IDR 15 billion
3	To increase Indonesia's cooperation with the South Pacific	IDR 15 billion
4	To manage security in the border regions of Australia and the South Pacific	IDR 5 billion
5	To increase security intelligence cooperation in the border regions of Australia and the South Pacific	IDR 5 billion

Source: Excerpt from Anggraini and Paolo (2019).

member countries, which narrows the space of ULMWP. This strategy seems to have been successful when Indonesia succeeded in dismissing ULMWP's application to become a member of the MSG as well as its willingness to obtain a higher status than the observer status it had held in the 2016 MSG Summit. The active and intense participation of the Indonesian delegation and representatives of Melanesia (North Maluku, Maluku, East Nusa Tenggara, West Papua, and Papua) ultimately succeeded in convincing the MSG leadership to disagree with the proposed ULMWP membership submission (Dewi, 2016).

The Pacific is one of the most aid-dependent regions in the world, with Australia as the leading donor followed by China, New Zealand, and other donor countries. Even though it faces the challenge of foreign aid in the region, Indonesia has never considered these major donors as its competitors in the provision of aid. Instead, Indonesia's aid serves as a compliment. It has committed to continue offering effective foreign aid to Pacific countries since the region is a significant part of its national interest. Indonesia's aid targets specific issues such as agriculture, fisheries, SMEs, food security, and general disaster mitigation, beginning with a small amount of aid but gradually seeing it increase (Ministry of Communication and Information Technology, 2016). In 2019, for example, the details of the total budget were IDR 60 billion (US$4,298,758.9443), as can be seen from Table 1.

Conclusion: An Indonesian Way of Securitizing Aid?

Foreign aid is a moral responsibility, but that responsibility does not always motivate the majority of donor countries in providing foreign assistance. There is clear evidence that foreign aid has dual motivations as both a tangible humanitarian

endeavor and a function of self-interest. Donor countries use foreign assistance without a coherent policy and clear objectives as a result of various demands.

The global war on terrorism or the international military campaign launched by the United States Government after the September 11 attacks has shifted the agenda of global security, resulting in new security concerns that have dominated foreign policy and impacted the foreign aid of many major donors. In this milieu, recipients have lost their "ownership" of the aid since the donors allocate their money for geostrategic interests and have less to do with providing human security, reducing poverty, and eliminating disease (Woods, 2005, p. 394). Indonesia, however, does not follow this trend because its foreign assistance is prioritized to secure its territorial integrity.

As a form of symbolic dominance, foreign aid is as an active agent of strengthening, mitigating, or even exacerbating the existing conditions of material inequality. This symbolic dominance reinforces the existence of social hierarchies, whose gifts are described as gentle invisible violence and are often not realized, especially by the recipient state. Although political motivation is a significant consideration for donor countries in providing foreign assistance, the logic and economic calculations are always included, at least to cover the real reason for the assistance. Foreign aid aims to overcome the crisis of recipient countries by encouraging economic growth and development there. However, it is not always the case that foreign aid is successful in overcoming the crisis; instead, foreign aid may worsen conditions in the recipient country. The motif of the donor country is a precondition that determines the success or failure of foreign aid in overcoming crises in the recipient countries, and is defined by strategic benefits. When the strategic benefits of providing aid are substantial, it becomes ineffective because donor governments cannot credibly enforce their conditions for economic reform (Bearce and Tirone, 2010, p. 838). Foreign aid is often seen as a component of diplomacy and as a sophisticated instrument of control. If donor countries have considerable strategic benefits, aid will then be followed by an intervention from donor countries to recipient countries. The chance for recipient countries to allocate aid in the context of economic growth and development becomes small and even impossible because donor countries will not create enabling conditions for the recipient country to experience economic reform.

In order to maintain its territorial integrity, Jakarta has continuously improved its diplomatic efforts to thwart any attempt by the OPM to gain external support. The Suharto regime incorrectly viewed the Papuan struggle as one of the secession movements, despite the fact it has been a separatist group from the beginning. The movement has been using "guerilla diplomacy" to launch its independence campaign and raise international sympathy, especially among the people of Pacific countries.

However, Indonesia saw Papuan separatism as a domestic affair and wished to ensure that it did not become "internationalized." The conflict looked promising in the late 2000s for the separatists with Indonesia's "more aid for the Pacific" formula. However, Indonesia stopped this formula through the expansion and deepening of existing relationships with these countries into mutually beneficial relationships in order to secure its interests in the Pacific region.

Indonesia expects its Eastern neighbors to be stable, prosperous, and friendly, and it has been able to achieve this through development assistance which benefits both parties. The role of Indonesia is significant because Indonesia has the capacity to provide assistance suitable for the need of the Pacific countries. The opening of the Eastern door is aimed at silencing separatist groups who are still struggling to secede from Indonesia by sending a strong message that the region is now under its grip. The aid has proven to be successful in addressing the country's poor image in the region and, to a large extent, it has been able to successfully play its "ethnic card" and status as an emerging donor and a member of G20. Understanding its closest neighbors is vital in the maintenance of good neighborhood relations. However, in establishing relations with Pacific countries, diplomatic manners are often more important than the substance of the relationship itself. Therefore, there is a need to develop "non-formal" pillars in approaching these countries in any diplomatic relations.

Acknowledgments

We wish to thank our former student, Moch. Arief Setiawan, for helping us in the data collection.

References

Andhika, D. (2015). *Babak Baru di Pasifik Selatan* [New chapter in South Pacific]. Retrieved from http://www.mediaindonesia.com/news/read/5030/babak-baru-di-pasifik-selatan/2015-06-30#.

Anggraini, A. D., & Paolo, B. (2019). *Bantuan Indonesia untuk Negara Pasifik Selatan* [Indonesian assistance to the South Pacific country]. Retrieved from http://indonesiabaik.id/infografis/bantuan-indonesia-untuk-negara-pasifik-selatan.

Bayram, A. B. (2017). Aiding strangers: Generalized trust and the moral basis of public support for foreign development aid. *Foreign Policy Analysis*, *13*(1), 133–153. doi: 10.1093/fpa/orw008.

Bearce, D. H., & Tirone, D. C. (2010). Foreign aid effectiveness and the strategic goals of donor government. *The Journals of Politics*, *72*(3), 837–851.

Carle, M. (2015). *Emerging donors and development cooperation: Thailand and Malaysia*. Retrieved from http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=7855312&fileOId=7855314.

Deplu RI. (n.d.). *Indonesia Secara Resmi Diterima Sebagai Negara Mitra Wicara Organisasi Forum Kepulauan Pasifik* [Indonesia officially admitted as dialogue partner in PIF] (Press Release No. 21/PR/V/01). Retrieved from https://kemlu.go.id/portal/id.

Dewi, S. (2016). *ULMWP fails in becoming Full Member of Melanesian Spearhead Group*. Retrieved from www.kemlu.go.id/en/berita/Pages/ulmwp-fails-msg-full-membership.aspx.

Dugis, V., Susilo, I. B., Salamah, L., Wardhani, B. L. S. W., Indonesia Badan Penelitian dan Pengembangan Masalah Luar Negeri, & Universitas Airlangga. (2001). *Kebijakan RI di Pasifik, Upaya Mencegah Separatisme di Irian Jaya* [RI's policy in the Pacific, efforts to prevent separatism in Irian Jaya]. Surabaya and Jakarta, Indonesia: Universitas Airlangga and Indonesian Ministry of Foreign Affairs.

Fardah. (2015). Melanesian festival celebrates cultural diversity. *Antara News*. Retrieved from https://en.antaranews.com/news/101211/melanesian-festival-celebrates-cultural-diversity.

Fardah. (2016). Indonesia strengthens ties with Pacific "good friends." Retrieved from https://asiapacificreport.nz/2016/04/08/indonesia-strengthens-ties-with-its-pacific-good-friends/.

FORUM Communique. (2001). *Thirty-Second Pacific Islands Forum*. Retrieved from http://www.forumsec.org/wp-content/uploads/Communiqu%C3%A9/2001%20Communiqu%C3%A9-Nauru%2016-18%20Aug.pdf.

Gani, A. (2006). Pacific Island countries high per capita foreign aid requirement. *Journal of International Development*, *18*(2), 285–292.

Hadipranowo, M. S. (1991). Upgrading of bilateral links between Indonesia, Papua New Guinea and the South Pacific countries. *Jurnal Luar Negeri*, *18*, 56–65.

Hattori, T. (2001). Reconceptualizing foreign aid. *Review of International Political Economy*, *8*(4), 633–660.

Hayward-Jones, J. (2015, May 13). Australia's Pacific aid budget spared from serious cuts. *The Interpreter*. Retrieved from http://www.lowyinterpreter.org/post/2015/05/13/Australia-aid-budget-Pacific-spared-serious-cuts.aspx.

Hopkins, R. (2000). *Political economy of foreign aid*. Retrieved from http://www.swarthmore.edu/SocSci/rhopkin1/research/PolEconFA.pdf.

Indonesia creates development agency to aid neighbors. (2019). *Japan Times.* Retrieved from https://www.japantimes.co.jp/news/2019/10/19/asia-pacific/indonesia-creates-development-agency-aid-neighbors/#.Xc4crdUzaos.

International Labour Organization. (n.d.). *South-South and Triangular Cooperation*. Retrieved from https://www.ilo.org/pardev/south-south/lang–en/index.htm.

Jakarta Commitment. (2009). *Jakarta Commitment: Aid for development effectiveness*. Retrieved from http://mdtf.undp.org/document/download/9714.

KBRI Port Moresby [Embassy of the Republic of Indonesia in Port Moresby, Papua New Guinea], & Kementerian Luar Negeri [Ministry of Foreign Affairs of the Republic of Indonesia]. (2015). *Indonesia Tindak lanjuti Komitmen Bantuan untuk Negara-negara Pasifik Selatan* [Indonesia following up on aid commitments to South Pacific countries]. Retrieved http://portal.kemlu.go.id/Pages/News.aspx?IDP=7552&l=id.

Kementerian Luar Negeri [Ministry of Foreign Affairs of the Republic of Indonesia]. (2014). *Indonesia Tegaskan Komitmen Pererat Kerjasama dengan Negara-negara Kepulauan Pasifi* [Indonesia affirms commitment to strengthen cooperation with Pacific Island countries]. Retrieved from http://www.kemlu.go.id/id/berita/Pages/IndonesiaTegaskan KomitmenPereratKerja SamadenganNegaranegaraKepulauanPasifik.aspx.

Kilby, C. (1999). Aid and sovereignty. *Social Theory and Practice*, *25*(1), 79–92. Retrieved from https://www.jstor.org/stable/23560322.

Klingebiel, S. (2014). *Development cooperation: Challenges of the new aid architecture*. New York, NY: Palgrave Macmillan.

Kompas. (2000). *Wapres: PNG Dukung Integritas RI* [Vice President: PNG supports Indonesian sovereignty]. Retrieved from www.kompas.com/kompas-cetak/0009/18/nasional/wapr06.htm.

Kompas. (2001a, August 21). *PIF Dukung Otonomi Khusus Irja* [PIF supports Irian Jaya special autonomy].

Kompas. (2001b, August 23). *Indonesia Tawarkan Hubungan Diplomatik dengan Negara-negara Pasifik Selatan* [Indonesia offers diplomatic relations with South Pacific nations].

Lawson, S. (2016). West Papua, Indonesia and the Melanesian Spearhead Group: Competing logics in regional and international politics. *Australian Journal of International Affairs*, *70*(5), 506–524. doi: 10.1080/10357718.2015.1119231.

Lin, E. (2019). How a West Papuan activist snuck into a UN meeting to deliver a direct message to Michelle Bachelet. *SBS News*. Retrieved from https://www.sbs.com.au/news/how-a-west-papuan-activist-snuck-into-a-un-meeting-to-deliver-a-direct-message-to-michelle-bachelet.

Martinez, J. (2016). *Emerging nations: BRICS and MINT*. Retrieved from http://www.socsci.uci.edu/globalconnect/webppts/GlobalComp4Power/02%20Emerging%20Nations.pdf.

Marx, A., & Soares, J. (2013). *South Korea's transition from recipient to DAC donor: Assessing Korea's development cooperation policy*. Retrieved from https://poldev.revues.org/1535.

Maulidiah, S. N. (2013). *Indonesia's South-South and Triangular Cooperation: Our stories, experience and on moving forward*. Retrieved from https://asiafoundation.org/resources/pdfs/IDSitiNugrahaMauludiah.pdf.

Ministry of Communication and Information Technology. (2016, December 2). RI and the Pacific: A history of cooperation. *The Jakarta Post*. Retrieved from https://www.thejakartapost.com/adv/2016/12/02/ri-and-the-pacific-a-history-of-cooperation.html.

Ministry of Foreign Affairs of Republic of Indonesia. (2015a). *Indonesia contributes to Melanesian Spearhead Group*. Retrieved from https://www.kemlu.go.id/en/berita/Pages/Indonesia-Contributes-to-Melanesian-Spearhead-Group-through-Cooperation-in-Various-Fields.aspx.

Ministry of Foreign Affairs of Republic of Indonesia. (2015b). *Rencana Strategis KEMLU 2015-2019* [2015-2019 Ministry of Foreign Affairs strategic plan]. Jakarta, Indonesia: Kementerian Luar Negeri Republik Indonesia.

National Coordination Team of SSTC. (2015). *Annual Report of Indonesia's South-South and Triangular Cooperation 2014*. Retrieved from http://open_jicareport.jica.go.jp/pdf/12315693.pdf.

OECD Library. (2014). *Making development co-operation more effective: 2014 Progress Report* (Progress Report, Chapter 5: Country actions to implement the Busan commitments). Retrieved from http://www.oecd-library.org/docserver/download/4314021ec009.pdf?expires=1476875129&id=id&accname=guest&checksum=3518B0142730B3782C0732C7373359E3.

Pacific Institute of Public Policy. (2008). *MSG: Trading on political capital and Melanesian solidarity.* Retrieved from www.pacificpolicy.org/wp-content/uploads/2012/05/D02-PiPP.pdf.

Pacific Islands Development Forum. (2014). Keynote address at the Second Summit of the Pacific Islands Development Forum. Retrieved from http://pacificidf.org/his-excellency-prof-dr-susilo-bambang-yudhoyono-president-of-the-republic-of-indonesia-keynote-address-at-the-second-summit-of-the-pacific-islands-development-forum/.

Pacific Islands Development Forum. (2015). *What is Pacific Islands Development Forum?* Retrieved from http://pacificidf.org/what-is-pidf/.

Pacific nations want UN to investigate Indonesia on West Papua. (2017). *SBS News*. Retrieved from https://www.sbs.com.au/news/pacific-nations-want-un-to-investigate-indonesia-on-west-papua.

Picard, L. A., Groelsema, R., & Buss, T. F. (2008). *Foreign aid and foreign policy: Lesson for the next half-century.* London, UK: M.E. Sharpe and National Academy of Public Administration.

Pramono, S. (2016, October 28). With Indonesia, MSG benefits from Asian Century. *The Jakarta Post.* Retrieved from www.thejakartapost.com/academia/2016/10/28/with-indonesia-msg-benefits-from-asian-century.html.

Pryke, J. (2013, September 2). The Pacific's aid boom [Blog post]. *Devpolicy@ANU*. Retrieved from http://devpolicy.org.

Putri, W. D. (2015, October 22). Festival Melanesia, Kenalkan Keberagaman Indonesia. *Republika*. Retrieved from http://republika.co.id/berita/gaya-hidup/travelling/15/10/22/nwm9vi359-festival-melanesia-kenalkan-keberagaman-indonesia.

Radio ABC. (2014). *Indonesia pledges $20m to help Pacific nations fight climate change*. Retrieved from http://www.abc.net.au/news/2014-06-19/an-sby-in-fiji-pidf/5535892.

Radio Australia. (2000). *Wapres Akan Resmikan Patung Bung Karno di PNG* [Vice President will officiate Bung Karno Statue in PNG]. Retrieved from www.radioaustralia.net.au/indonesian/2000-08-31/wapres-akan-resmikan-patung-bung-karno-di-png/795346.

Radio New Zealand. (2017). *Indonesia offers increased assistance to Samoa and Pacific.* Retrieved from https://www.radionz.co.nz/international/pacific-news/339662/indonesia-offers-increased-assistance-to-samoa-and-pacific.

Reilly, B. (2004). State functioning and state failure in the South Pacific. *Australian Journal of International Affairs*, *58*(4), 479-493. doi: 10.1080/1035771042000304742.

Saideman, S., Dougherty, B. K., & Jenne, E. K. (2005). Dilemmas of divorce: How secessionist identities cut both ways. *Security Studies*, *14*(4), 1-30. doi: 10.1080/09636410500468800.

Shibuya, E. (2003). *The problems and potential of the Pacific Islands Forum*. Retrieved from http://apcss.org/Publications/Edited%20Volumes/RegionalFinal%20chapters/Chapter7-Shibuya.pdf.

Siliwanti, R. (2011). *Indonesia South-South and Triangular Cooperation*. Retrieved from https://www.cbd.int/financial/southsouth/Indonesia-south.pdf.

SSC-Indonesia. (2015). *Indonesia's Capacity Building Program for Pacific*. Retrieved from http://ssc-indonesia.org/ksst/wp-content/uploads/2015/07/Leaflet-Pacific-Update2.pdf.

Tahalele, M. (2016). *The changing role of Indonesia in development cooperation: The shifting rhetoric of South-South cooperation*. Retrieved from http://devpolicy.org/2016-Australasian-aid-conference/Presentations/Day-2/4b-Aid-to-and-from-Asia_Tahalele.pdf.

The Asia Foundation. (2014). *The changing aid landscape in East Asia: The rise of non-DAC providers*. Retrieved from https://asiafoundation.org/resources/pdfs/ChangingAidLandscapeinEastAsia.pdf.

The United Nations Development Programme (UNDP). (2015). *UNDP Indonesia — Brief: South-South and Triangular Cooperation in Indonesia*. Retrieved from http://www.id.undp.org/content/dam/indonesia/2015/brief/SSC-briefUNDPformat.pdf.

Trinidad, D. (2014). *South-South Cooperation in Southeast Asia and the role of Japan* (V.R.F. Series No. 489). Tokyo, Japan: Institute of Developing Economies, Japan External Trade

Organization. Retrieved from https://www.ide.go.jp/library/English/Publish/Download/Vrf/pdf/489.pdf.

Ulaş, L. (2016). Cosmopolitanism, self-interest and world government. *Political Studies*, *64*(1), 105-120. doi: 10.1177/0032321715624424.

Usman, A. (1994). Indonesia dan Pasifik Selatan [Indonesia and the South Pacific]. In B. Bandoro (Ed.), *Hubungan Luar Negeri Indonesia Selama Orde Baru* [Indonesia's foreign relations during the new order] (pp. 187–215). Jakarta, Indonesia: Center for Strategic and International Studies.

Vanhanen, T. (1991). *Politics of ethnic nepotism: India as an example*. New Delhi, India: Sterling Publishers.

Waluyo, A. (2014). *SBY Kunjungi Fiji Untuk Jelaskan Masalah Papua* [SBY visits Fiji explaining Papua issue]. Retrieved from www.voaindonesia.com/a/sby-kunjungi-fiji-untuk-jelaskan-kondisi-papua/1938483.html.

Walz, J., & Ramachandran, V. (2011). *Brave new world: A literature review of emerging donor the changing nature of foreign assistance*. Retrieved from http://www.cgdev.org/files/1425691_file_Walz_Ramachandran_Brave_New_World_FINAL.pdf.

Wangge, H. Y. R. (2016). Explaining the effectiveness of Indonesia's foreign policy toward the Papuan issue in a South Pacific region. In *Proceedings of International Conference on Contemporary Social and Political Affairs (ICOCSPA) 2016* (pp. 266–273).

Wardhani, B. (2015). Quo vadis Melanesian Spearhead Group? *Global & Strategis*, *9*(2), 190–206.

Wasserman, G. (1983). The foreign aid dilemma. *The Washington Quarterly*, *6*(1), 96–106. doi: 10.1080/01636608309477588.

Woods, N. (2005). The shifting politics of foreign aid. *International Affairs*, *81*(2), 393–409.

Wyeth, G. (2017, June 5). For Pacific Island states, climate change is an existential threat. *The Diplomat*. Retrieved from https://thediplomat.com/2017/06/for-pacific-island-states-climate-change-is-an-existential-threat/.

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

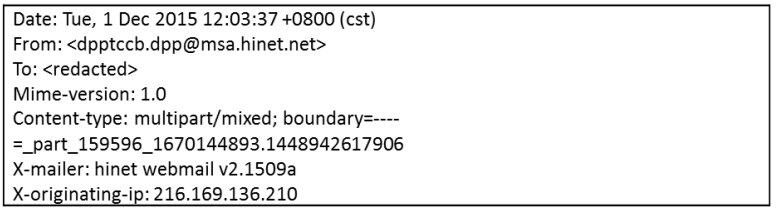
It can be argued that the integration of *weishe* by the PLA within its cyber operations is central to its strategy of pursuing the Chinese dream of reunification with Taiwan, tightening its political control in Hong Kong, and its assertion of its sovereignty in the South China Sea. This section shall 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).

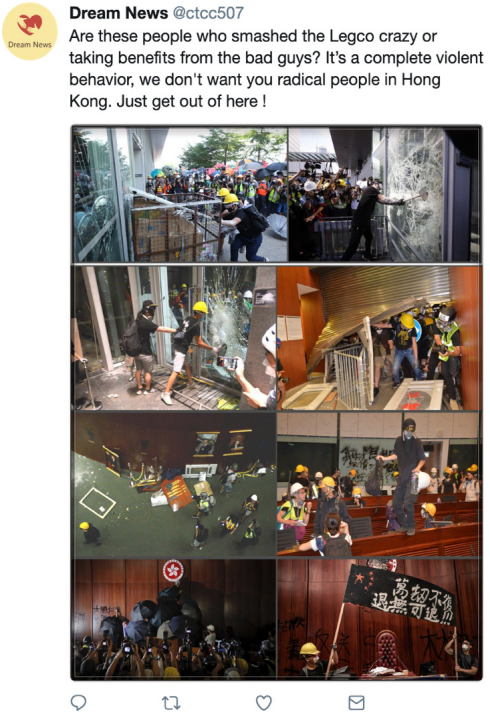
Source: From Kumar (2019).

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.

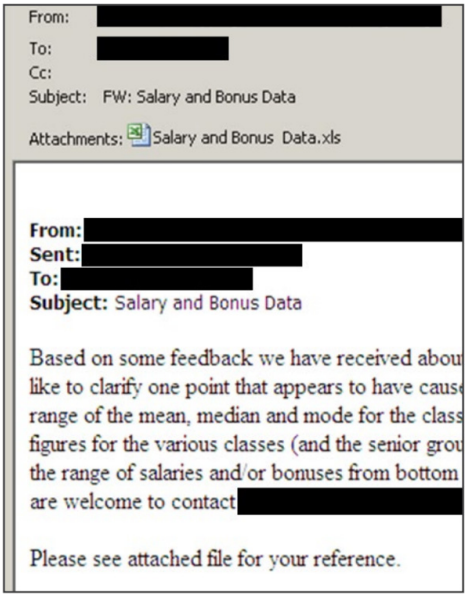
In recent years, growing scrutiny against China's "gray-zone strategy" in the contested waters has dominated mainstream media and policy discussions. However, very little attention has been devoted to China's deployment of cyber coercion to further its interests in the resource-rich waters. China's tools 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.

Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs
Vol. 56, No. 3 (September 2020) 2040011 (20 pages)

DOI: 10.1142/S1013251120400111

Evolving Toward a Balanced Cyber Strategy in East Asia: Cyber Deterrence or Cooperation?

HON-MIN YAU

This paper investigates the limits of implementing a cyber deterrence strategy in East Asia. Given that national security documents from both Taiwan and Japan indicate the need to deter state-sponsored cyberattacks, there is very little literature that empirically and theoretically investigates the utility of such an approach in this region. This paper looks into the various deterrence constructs and argues that none of them can be implemented without problems. The paper looks further into a deeper level of the conceptual issues upon which deterrence thinking is based and argues that an alternative strategy promoting regional cooperation is not only possible but also desirable in the current political climate. It is later concluded that looking for a one-size-fits-all solution is idealistic, and policymakers should develop security countermeasures that align with the threats posed by the actors they wish to confront.

KEYWORDS: **Deterrence theory; security policy; kinetic cyberattacks; cybersecurity; international relations.**

* * *

論 In today's wired world, both public and private organizations are relying on cyberspace for everything from financial transactions to military movement. States and societies are increasingly dependent on information; businesses are quickly promoted, and ideas are freely shared. Cyberspace has become an intrinsic part of our daily activities. However, the water that bears a boat is the same that swallows it up. Traditional threats, namely nations and states, are now exploiting this non-traditional means. The general public's reliance on digital

HON-MIN YAU (姚宏旻) is an Assistant Professor at the Graduate Institute of Strategic Studies (GISS), War College, National Defense University, Taiwan. His research interests focus on global security and national security policy. He can be reached at <cf22517855@gmail.com>.

technology has created new security challenges for the survival of states, and cybersecurity has been considered by many countries as an essential issue impacting their national security.

The following well-known events further attest to this observation. In 2007, Estonia became the victim of massive cyberattacks during a political dispute over relocating a Soviet-era Memorial Statue within the capital city, Tallinn (Bright, 2007). Later in 2008, Georgia suffered a barrage of cyberattacks during Russia's intervention during the independence movements of two autonomous Georgian regions (Korns & Kastenberg, 2009). In 2010, a malicious computer worm, Stuxnet, disrupted Iranian nuclear development for a couple of years by creating kinetic destruction to centrifuges in its highly secured Natanz, a uranium enrichment facility (Farwell & Rohozinski, 2011). The software was praised as the first "fire and forget" cyberweapon (Milevski, 2011, p. 64). Recently in 2017, it was reported by the *New York Times* that the US had conducted an anti-ballistic missile program via cyber means, known among policymakers as "left of launch," to disable North Korea's nuclear ballistic ambition (Broad & Sanger, 2017). As such sophisticated forms of cyber threats are prevalent, state-sponsored cyberattacks with the potential to deliver kinetic and physical destruction are considered an important issue in national defense policymaking. Hence, this paper plans to investigate how states can deal with these challenges in cybersecurity.

As the interest of states in leveraging evolving cyberwarfare techniques has grown significantly, various countries are devoting resources to making themselves cyber-sophisticated (Stoddart, 2016, p. 833). Policymakers are engaging in applying the concept of "deterrence" in cyberspace in keeping with this trend. In East Asia, this tendency toward security enhancement has caught the attention of Taiwan and Japan.

Upon the inauguration of Taiwan's Tsai Ing-wen administration in 2016, the government immediately established the Department of Cybersecurity in the Executive Yuan to step up Taiwan's cyber defense efforts ("Cabinet Forms," 2016; Executive Yuan, 2016). In 2017, Taiwan's Ministry of National Defense (MND) established the Information, Communication, and Electronic Warfare Command to build offensive capabilities to counter China's cyberattacks (Huang & Liu, 2017; Ministry of Foreign Affairs [MOFA], 2017). Taiwan also passed the Information and Communication Security Management Act in May 2018 to tighten up its public and private partnership in cybersecurity (Lin, 2018), and in September 2018, the National Security Council published its first *National Cybersecurity Strategy Report* promoting "cybersecurity as the national security" (Office of the President, 2018).

By July 2019, the National Security Act had been modified to provide a legal mandate for government agencies, such as the military, to protect Taiwan's cyberspace (Legislative Yuan, 2019). As was later pointed out by *The 2019 National Defense Report*, Taiwan plans to establish "credible cyber offense and defense capability" (MND, 2019, p. 69) as "the first layer of deterrent force" (Legislative Yuan, 2019, p. 211) to support the military strategy of "resolute defense, multi-domain deterrence" (MND, 2017, p. 38).

At the same time, Japanese Prime Minister Shinzō Abe has continuously called for better cyber capabilities throughout his administration. His and Japan's first *National Security Strategy* (NSS) in 2013 identified cyber threats as a significant risk for the global commons (Prime Minister's Office, 2013). His government passed *The Basic Act on Cybersecurity* in 2014 to create a mandate for the government to form a cybersecurity strategy. The latest *Cybersecurity Strategy* in 2018 highlighted the role of the Self-Defense Force (SDF) and designated an independent section to emphasize the need for "enhancing deterrence capabilities" against cyberattacks (National Center of Incident Readiness and Strategy for Cybersecurity, 2018). In addition, the current *National Defense Program Guidelines* (NDPG) (Japanese Government, 2018b) and the *Medium Term Defense Program* (MDP) (Japanese Government, 2018a) have called for the need to deter any cyberattacks, emphasizing the necessity of strengthening the "capability to disrupt . . . opponents' use of cyberspace for the attack" during conflicts against Japan. Japan's sense of insecurity in cyberspace is a reaction to certain developments in geopolitical competition, including longstanding territorial disputes in the East China Sea, and it was reported by *The Japan Times* on December 21, 2018 that the country's Ministry of Foreign Affairs had urged China to take "responsible" actions against cyberattacks in association with Chinese state organs ("Japan Slams," 2018).

Given that both Taiwan and Japan see themselves as under the threat of cyberattacks from China, it will be beneficial for this study to explore the strategic designs of both countries. However, the current literature provides little analysis of the use of a deterrence strategy in this East Asian security context. Furthermore, while policy documents from both Taiwan and Japan seem to suggest a plan for deterrence against cyberattacks, neither has offered specific statements or arguments regarding the utility of such a stance. As both countries are encountering common cyber threats from China, the overall aim of this paper is to assess the strategic value of a deterrence framework in cyberspace. Hence, this paper investigates the extent to which a deterrence strategy could deter malicious activities in the cyber domain and the possible implications within the East Asian context.

Deterrence Theories

Problems of Using Nuclear Deterrence Thinking in Cyberspace

In the discipline of International Relations (IR), deterrence is an old practice inherited from the Cold War. At that time, great powers threatened each other with nuclear force to manipulate the decision-making process of their adversaries. The use of a "threat" by one party could influence a rational actor's cost and benefit calculations, and any rival could be psychologically convinced that unacceptable losses could outweigh any possible gains under a certain course of action (Geers, 2010; Jervis, Lebow, & Stein, 1989).

However, the past literature has questioned the effectiveness of deterrence as suggested by nuclear strategists (Libicki, 2009), and one of the most significant limitations in cyberspace is the problem of attribution. Attribution in cybersecurity refers to the ability to locate the identity of attackers. However, users in cyberspace very often enjoy the advantage of being anonymous. Since we do not know who are the malicious actors behind a cyberattack, whom should we deter (Glaser, 2011)? Besides, if the perpetrators of cyberattacks are a terrorist group instead of a "rational" state actor, the fundamental assumption for a classic (nuclear) deterrence strategy would be unsustainable since the logic of the attackers in terms of a cost–benefit calculation could be quite distinct from that of a state actor. Furthermore, when suffering cyberattacks, the scale of the damage is not immediately estimable. To what extent should a state respond in order to deliver a credible threat based on uncertainty (Rid & Buchanan, 2015)? There are also complicated issues involving the legality of a cyber response (Yau, 2015) and the liability of potential spillover effects to other domains such as liberty, rights, and trust (Jasper, 2015). In addition, as cyber capabilities are hard to quantify and gauge, most of the literature talks about cyber power in the international system without explaining how it is measured (Yau, 2019b). Due to these various limitations and our inability to effectively deter attackers in cyberspace, Martin Libicki concludes in *Cyberdeterrence and Cyberwar* by saying that "Cyberretaliation — with all its difficulties — should not be the only response in the repertoire" (Libicki, 2009).

New Deterrence Variants in Cyberspace

Classic deterrence theorizing during the nuclear age places an excessive emphasis on credibly presenting the "means" of punishment, instead of thinking about how to achieve the "ends" of deterrence by altering an adversary's perception.

This is to say that if the essence of a deterrence strategy is to influence a rival's mental calculations and psychological awareness, such an "end" could in fact be achieved by means other than a direct threat. As the theorizing of deterrence strategies focuses on affecting an adversary's cost and benefit calculations, there are in general two approaches that can be used to achieve deterrent effects. One is "deterrence by punishment," which means increasing the "costs" in an aggressor's calculation formula, and the other one "deterrence by denial," which intends to reduce the potential "benefits" of an act of aggression (Mazarr, 2018; G. H. Snyder, 1959).

However, as explained in the previous sub-section, the conventional argument is that a deterrence strategy is less effective in the cyber domain as it is unable to locate the identity of the attackers. It thereby offers plausible deniability for malicious actors, which can fundamentally constrain the utility of the strategy. Nevertheless, the problem of attribution is now being considered a challenge rather than an impossibility due to advancements in technology (US DoD, 2015, pp. 11–12). For example, a conclusion in regard to attribution can be reached by investigating the code of the malware and software infrastructure used by attackers, as it may contain some tool marks that can help identify the attackers (Ghosh, 2016; Rid & Buchanan, 2015). Certain tactics, techniques, and procedures are also often repeatedly used by the same group of hostile actors (Berghel, 2017). The literature indicates that many hacking activities are publicly attributed to specific actors (Rid & Buchanan, 2015; Yau, 2019a), and the US Office of the Director of National Intelligence in September 2018 stated in its official report, *A Guide to Cyber Attribution*: "Establishing attribution for cyber operations is difficult but not impossible" (Office of the Director of National Intelligence, 2018). Undermining the advantage of plausible deniability in cyberspace has promoted the cottage industry of conceptual theorizing for deterrence in cyberspace. Hence, when thinking about the security context of cyberspace in this framework, five methods are currently referred to with frequency in the literature, and they are introduced below.

The first approach is "cyber defense." As an approach to deterrence through denial, cyber defense intends to fortify one's cyberspace. This method has been a standard practice for nations and states, whereby they make a malicious actor consider that the potential gains are not worth the resources and time invested. However, given the perception that this method is limited in its effectiveness, as exemplified by the prevalence of cyberattacks, many countries are looking into more aggressive approaches.

The international community is looking into the approach of deterrence by punishment. This approach comprises the other four methods, which are "cyber offence,"

"active cyber defense," "entanglement," and "norms" to increase the cost of initiating cyberattacks. Cyber offence refers to using cyber means to punish malicious perpetrators. While cyber offence has the negative connotation of being considered an aggressive act and destabilizing to international peace (Hathaway, Crootof, Levitz, & Nix, 2012), some studies have attempted to justify the practice by stating that active cyber defense, commonly known as "hack back," is in line with the right to self-defense as specified in the United Nations (UN) charter (Rosenzweig, Bucci, & Inserra, 2017). In addition to the three methods mentioned above which aim to shape an actor's perception of the costs behind cyberattacks, Joseph Samuel Nye, Jr. proposes stretching cyber deterrence to include "entanglement" and "norms" as two alternative methods (Nye, Jr., 2017). Entanglement refers to an actor's awareness that while interconnectivity makes initiating a cyberattack relatively easy and cheap, the same characteristics can be exploited by an adversary. Deterrence by norms is similar to the "naming and shaming" approach in regard to the nuclear taboo, and it requires the international community's development of norms in cyberspace.

Empirical Challenges of Cyber Deterrence in East Asia

When we examine these five methods in an East Asian context, we will discover that each of them is either insufficient or lacks certain capabilities when compared with current empirical developments.

Traditionally, an argument for the failure of deterrence in cyberspace was based on the fact that low-cost readymade intrusion tools were widely available for non-state actors, but Joseph Samuel Nye, Jr. argues that deterrence by "defense," implemented by a relatively resource-rich state, can deny non-state actors such low-skilled intrusions (Nye, Jr., 2017). Given that the starting point of this paper is to understand how Taiwan and Japan can deter China-sponsored malicious cyber activities, the effectiveness of a deterrence strategy against non-state actors would not be a point of contention within this paper. However, what we can take from this argument is that a purely "cyber defense" method is insufficient to deal with a sophisticated actor with high cyber skills, and China seems to fit into this profile in East Asia. Taiwan's *2019 National Defense Whitepaper* states that under the guideline of "Integrated Network Electronic Warfare (INEW)," the PLA continues to develop various platforms to attack networks and information within our essential organization (MND, 2019, p. 40), and the Japanese NDPG has also stated that: "[China] is rapidly advancing capabilities in cyber and electromagnetic domains with which to disrupt opponent's command and

control" (Japanese Government, 2018b, p. 5). Due to geopolitical reasons, both Taiwan and Japan appear to have identified China as a major cyber threat, and they feel the need to enhance their cyber postures.

However, this does not mean that strategies of "cyber offence" will be useful because the success of this method depends on the opponent being persuaded by changing its perception of another actor's cyber capabilities. Three crucial factors of capabilities, credibility, and communicating a threatening message to the challenger are required to ensure the success of this method (Morgan, 2003, pp. 15–20). Among them, credibility is the most important consideration. Thomas Schelling noted that: "... to *persuade* enemies or allies... It requires projecting intentions. It requires *having* those intentions, even deliberately acquiring them, and communicating them persuasively to make other countries behave." With regard to the subject of this paper, this relates to how Taiwan and Japan can demonstrate offensive cyber capabilities to creditably dissuade China from continuing its hostile cyber activities both in word and practice. While the wording of policy documents in both Taiwan and Japan is strong and unquestionable, it is more about how to demonstrate their offensive capabilities. But this scenario needs to be more than just an act of cyber vandalism in order to be credible; it is very likely that it should be a case of Stuxnet-level demonstration.

The other consideration of "cyber offence" is that such deterrence through the use of a punishment strategy needs to penetrate through China's current cyber defense in order to be credible by demonstrating a use case within China's Great Firewall. However, if both Taiwan and Japan demonstrate such intrusive cyber capabilities by delivering kinetic destruction either within or outside Chinese cyberspace, the effect could likely backfire and damage the information and communications technology (ICT) reputations of both countries as exemplified in the debate over the information security (Infosec) risks of Huawei's 5G technology (Chee, 2019) and the international backlash against China's surveillance equipment exports from companies like Hikvision and Dahua Technology (Dai, 2019). As a reputation of trust in the ICT industry is an essential prerequisite for business success, cyberwarfare capabilities can spill over to the economic domain. The development of offensive cyber capabilities will inevitability sacrifice the economic security of both countries.

With these concerns in mind, a strategy of "active cyber defense" or a second-strike capability seems to be less troublesome. However, "active cyber defense" is probably more of a doctrinal issue, as the credibility of cyber capabilities is still crucial. Such a strategy is similar to a "cyber offence" method, and Taiwan and Japan still need to demonstrate a credible capacity for the success of this "active cyber defense," which ironically faces the same concerns as "cyber offence." In addition, due

to the high possibility of the disruption or destruction of civil networks during wartime, the success of a second strike capability in cyberspace implies the forward deployment of a Trojan horse or logic bomb on an adversary's information systems during peacetime (Clarke & Knake, 2011), which ironically presupposes an act of aggression that could potentially arouse political accusations and even create increased insecurity for the region. While Bernard Brodie argued that the purpose of deterrence is to shift the mission of military force from winning wars to preventing them, on the contrary, "active cyber defense" has the opposite potential of conflict escalation (Brodie, Dunn, Wolfers, Corbett, & Fox, 1946).

Furthermore, the conditions for adopting deterrence by "entanglement" are not sufficient yet in East Asia. When talking about nuclear deterrence, Richard Ned Lebow stated: "To the extent that deterrence worked, most of the credit should go to **self-deterrence** [emphasis added], reinforced by mutual recognition that a nuclear war could — indeed almost certainly would — result in mutual destruction" (Lebow, 2005). Hence, "entanglement" is often called "self-deterrence," and it requires China's self-awareness in recognizing that cyberattacks could be exploited by it and its adversaries and deliver destructive effects both within China and beyond. However, from the perspective of policy documents specified in Taiwan and Japan, they do not observe that China is concerned about cyber entanglement; otherwise, there would be no need for them to step up the cyber postures of both countries. It is very likely that Chinese telecom companies are all state-owned, and this environment allows China to have full control of network traffic via state-controlled critical communication nodes (Yau, 2018). Western countries rarely enjoy the same capabilities due to limited access to privately-owned infrastructures. Hence, China's Great Firewall provides relatively better security for China's cyberspace than other Western countries since such an on-path system can interfere with both inbound and outbound traffic directly through injection, redirection, and suppression. In other words, the "World Wide Web" in China is still the "China Wide Web."

In addition, the effectiveness of deterrence by "norms" is still questionable and yet to be defined. Just like Stephan Walt's argument in 1998 that there are many analytical perspectives on IR issues, attitudes toward appropriate conduct in cyberspace are also those of "one world, many theories" (Walt, 1998). Hence, proponents of a "tit for tat" strategy such as cyber deterrence using cyberattacks would argue that China will initiate cyberattacks on Taiwan and Japan regardless of what they do. They argue that safeguarding one's digital territory should rely on the enhancing of one's cyber capabilities instead of the goodwill of others. However, this line of thought ignores the possibility that international norms can sometimes constrain the behavior

of states. For example, the sovereignty of states used to be infrangible but is now redefined by international human rights laws, and whale hunting used to be legally justified as a state's right to harvest natural resources but is now reinterpreted as an act of endangering natural species. People attribute this norm building to the successful contribution of non-governmental organizations (NGOs) such as Amnesty International and the International Whaling Commission. While these NGOs do not have the command of military aircraft, tanks, and other forms of material power at the disposal of states, they can nevertheless shape international norms and make states refrain from taking unilateral action.

The above argument would suggest that deterrence through "norms" would presuppose the universal acknowledgment of appropriate cyber conduct by members of the international community. The question then would be, what are the norms for the activities of states in cyberspace? Unfortunately, institutions and norms in cybersecurity are only nascent (Buchanan, 2017, p. 22) and there is a lack of agreement on the standardization of such "norms." One commonly cited work is the Tallinn Manual, which specifies that, "cyber operations executed in the context of armed conflicts are subject to the law of armed conflict" (Schmitt, 2017, p. 375). The UN working group, the Group of Governmental Experts (GGE), only came to an initial understanding in 2015 that attacking critical infrastructure violated international laws such as the Law of Armed Conflict (UN General Assembly, 2015), but in 2017 it failed to agree on what constitutes a state's right to self-defense in cyberspace (Bowcott, 2017). While the international community is struggling to define the criteria for "armed attack" and "the use of force" in cyberspace (Lewis, 2015), the Open-Ended Working Group (OEWG), a new UN working group backed by Russia and China, was established in 2019 to offer an alternative forum for the shaping of cyber norms (UN General Assembly, 2019). As Russia has stated that "the practice of club agreements should be sent into the annals of history [in GGE]" (Kurowska, 2019, p. 9), it could be expected that the OEWG is destined to create tension with the interim cyber norms proposed by the GGE. Hence, this is not to deny the feasibility of deterrence through "norms," but the prerequisites for this strategy have not yet been realized. Speaking empirically, more time is still required for nations and states to converge their apparent contending positions.

The Conceptual Problems of Offensive Cyber Capabilities

The section above indicates that the utility of a deterrence strategy against state-sponsored cyberattacks is weaker than what policymakers have thought. Before there

is any apparent progress in deterrence through "entanglement" or "norms," nations and states are expected to compensate for insufficiencies in their "cyber defense" with continuous investment into their cyberwarfare capabilities, such as "cyber offence" or "active cyber defense," to reduce their sense of insecurity. Although they hope to use their offensive cyber capabilities to create a "deterrence by punishment" effect to dissuade their adversaries, there are more conceptual pitfalls that countries need to carefully consider.

First, developing an offensive cyber capacity is not cheap. It requires expansive and sophisticated collaboration in terms of talent, time, and intelligence and has no guarantee of actual success in future conflicts (Yau, 2019a). In the case of Stuxnet, people often pay attention to how this malware can exploit unknown software vulnerabilities in order to deliver kinetic destruction as it did in an Iranian nuclear facility. However, as programmers may make mistakes, so do hackers. It is often ignored that to ensure that Stuxnet worked without any coding mistakes, the developer must have acquired expansive nuclear centrifuges to make sure that the malware would work in the same environment (Broad, Markoff, & Sanger, 2011). Our tendency to use cyberwarfare to solve cybersecurity problems could be based on certain misconceptions of cyber weapons, and such a belief is reminiscent of the cult of the offensive during WWI and could have potentially tragic results (J. L. Snyder, 1984). The success of known cyber offensives is largely the result of poor management rather than a technologically determined advantage (Yau, 2019a), and empirical analyses have already indicated that the Stuxnet cyberattacks on Iran's nuclear facilities could have cost much more in terms of the offence than the defense (Slayton, 2017). While conventional wisdom may believe that cyberspace is an "offence-dominated" domain (Arquilla, 1996), winner of the inaugural NPS Foundation/U.S. Naval Institute Essay Contest Christopher Bartos argues in his work that cyber defense has a distinct advantage over cyber offence (Bartos, 2016). Hence, scholars have begun to be more critical of such a taken-for-granted conception, and many recognize that an offence strategy is only valid in a particular context (Lieber, 2014; Lindsay, 2013, 2015; Rid, 2013; Slayton, 2017).

Second, there is an unpredictable political cost that comes with the use of offensive cyber capabilities. A cyber weapon does not work like a drone or a missile, where the commander can know when and to what extent a target can be destroyed. It is also difficult for the attacker to predict the extent of collateral damage as they do not know what kind of systems are connected to the target network or where this cyber weapon will go in the interconnected network environment (Lewis, 2015). Due to the lack of reconnaissance capabilities for a battle damage assessment on the network, the

success of such cyber counterattacks is hardly measurable due to the problem of effect-based calculations on cyber weapons (Yau, 2019a). Hence, there is still doubt as to the effectiveness of offensive cyber capabilities in informing cyber defense.

Third, deterrence using a punishment strategy will inherently be an operation of countervalue that is incompatible with the current understanding of international laws. In the conventional conception of deterrence, counterforce and countervalue targeting are the two different courses of military action (Lutz, 1983). Countervalue targeting means holding targets appreciated by adversaries hostage in order to ensure their good behavior, and these targets are likely to be civilian populations or cities. Counterforce targeting is against the *sinew* of state power, and its targets refer to military forces or command and control facilities. In the East Asian context, as China can harvest a massive amount of Internet Protocol (IP) addresses, this creates a fundamental problem of target acquisition for Taiwan and Japan. It is questionable how Taiwan and Japan can conduct a counterforce strategy to pre-empt the unknown and anticipate the origin of future incoming cyberattacks from the People's Liberation Army's military information infrastructure which can be embedded in any Chinese public or private information facilities. It is also questionable how effective such a pre-emption would be even during a cyber conflict, as the attackers can constantly transfer from one IP address to another through the use of Zombie computers located anywhere in the world. This means that the only choice Taiwan and Japan have at their disposal is a countervalue operation, namely an attack on China's civil information infrastructure. However, this would imply attacking civilian targets in China, which is fundamentally against the enduring principles of military necessity along with distinction and proportionality in the Law of Armed Conflict. Such subtle differences are something that Taiwan and Japan need to think through carefully.

Finally, the advocates of developing offensive cyber capabilities not only overrate the utility of deterrence through punishment, but also often ignore the adverse effects that will result from such thinking. In the past, both Taiwan and Japan enjoyed enormous successes in the ICT industry due to their positive branding and credible reputations in terms of the security standards of their products. However, developing a capacity for cyberwarfare implies weaponizing this leading edge in ICT and leveraging their enterprises for the purpose of national defense, which is very problematic and counterproductive in a trust-based global ICT market. They face a unique cyber dilemma in which a state must sacrifice its economic security in order to enhance its offensive cyber capabilities, delivering a tactical advantage in cyberspace while resulting in a strategic loss in the real domain. While increasing one's cyber offence

capabilities cannot create disincentives to prevent war, it is however very likely to make the state more insecure (Yau, 2019a).

In short, the current conceptual scaffolding of cyber deterrence seems to limit our imagination of war and peace within the traditional security framework of the Cold War. The argument here is not that we should be utopian and campaign for political infeasibility, but rather that deterrence thinking in cyberspace is not only limited but also limiting, and investing in cyberwarfare capabilities has a huge potential to move from preventing a war into creating one. Developing a strategy other than pure deterrence thinking may provide a possible way ahead.

An Alternative Strategy: From Cyber Deterrence to Cyber Cooperation

While the above notion that the possession of offensive cyber capabilities can deliver a deterrent effect is much disputed, the unanswered question in this investigation is that other than a fortification strategy of deterrence by denial in peacetime, what more can states do?

In many aspects, cyberattacks are in fact similar to weapons of mass destruction (WMD) attacks delivered through ballistic missiles. Since a ballistic missile can be airborne-launched, submarine-launched, or land-based-launched (by fixed or mobile sites), and it is very challenging for defenders to know without proper intelligence where a ballistic missile is coming from and going to and what kind of payload it carries. Depending on its trajectory, this kind of attack can be quick and stealthy, and the attack often gives defenders very little time to react. Likewise, a cyberattack can come from public or private facilities either within or outside China. It can travel through multiple countries to conceal its identity before finally reaching its targets. Hence, the defense of these time-sensitive threats requires a collaborated intelligence and a well-coordinated response by surveillance sensors along their attacking trajectories. The prerequisite of a decent defense is good situation awareness, and security decisions depend on good intelligence. As a result, a key condition for fostering anything closer to credible deterrence in any form is the ability to respond to malicious cyberattacks (Lété & Pernik, 2017), and this ability to respond is based on a sufficient knowledge of malware signatures that includes what software vulnerabilities are used, where the malware was discovered before, what kind of platform this malware is targeting, and any potential known forensic evidence. Therefore, a purely national approach to cybersecurity is inadequate. Maximizing the available response time can

only be achieved with a close social network of information sharing in the form of a knowledge nexus embodying many countries in social and technical consultation from the moment that attacks are discovered.

Hence, an alternative strategy for East Asia would be a collaborative one in which like-minded countries with similar values and common threats cooperate in their technological development with the advancement of Infosec products, and share cyber intelligence by issuing malware reports and offering fixes for software vulnerabilities that are discovered. For a cyberattack to be successful, malware needs to exploit software vulnerabilities before they are spotted by defenders. Because a perpetrator's malware can only profit when a victim country is not aware of these software defects, the sharing of collected software vulnerabilities among countries can reduce the window of opportunity for attackers to exploit. These like-minded countries must also acknowledge when they cannot even agree among themselves and come up with arrangements for a positive cyber exchange; otherwise, how can they expect to have a progressive cyber world in which deterrence through "norms" and "entanglement" is likely to succeed?

However, this seems to be easier said than done, and it brings up another valid question. While cyberspace in its current state is anarchic without a stable structure to sustain the possibility of cooperation, how can we be sure that no one is cheating in this information sharing alliance and secretly stockpiling and weaponizing computer vulnerabilities? During the Cold War, security was achieved through the insurance of military security, and weapons designed for the purposes of both "offence" and "defense" were considered a means to an end. This has been termed "the symbolic ambiguity of weapons" (Booth & Wheeler, 2007). One state cannot make itself more secure without making another less so, and this problem is termed the "security dilemma." In cyberspace, however, offence and defense can sometimes be separated to eliminate ambiguity in the interpretations of cyber countermeasures. As Libicki argues, "most of what brings about cybersecurity cannot possibly make others less secure directly" (Libicki, 2016). For example, research and development investment into technologies without implications of "cyber offensive capabilities" such as encryption, authentication, access control, and comprehensive procedures could, in theory, maintain one's cybersecurity to an acceptable extent. While the above technologies are already well understood by academics, industries, and states as clearly non-threatening and defensive measurements, implementing a strategy to invest in such technological development has little chance of being misinterpreted by the international community (Yau, 2019a). So far, the most controversial tool for cyberspace may be commercial penetration testing software, which is deemed by some as being

capable of both offensive and defensive purposes. However, we should not ignore the fact that such tools are typically developed based on openly available vulnerabilities that are arguably not as cyber-sophisticated as Stuxnet. Hence, once the differentiation between offence and defense happens, as Robert Jervis once argued, it can permit cooperation among states (Jervis, 1978). Any defense cooperation should not simply be the wishful thinking of states, and Jervis's argument suggests that even when countries would like to cooperate, the symbolic ambiguity of weapons in a realist world could hinder such a possibility. Only when defense can be separated from offence will states be capable of understanding that their security partners will not defect or cheat in international cooperation.

In the future, one possible way forward is for like-minded countries to enhance and extend their cyber cooperation based on existing dialogs. Established in 1990, FIRST.org is the most well-known NGO on a global scale. It has been recognized as the senior, leading organization in coordinating international resources in computer security, and there are 330 organizations in 73 countries. In the Asia-Pacific region, the Asia Pacific Computer Emergency Response Team (APCERT) was initiated by the Japanese Computer Emergency Response Team/Coordination Center (JPCERT/CC) in 2002 to encourage international cooperation and support, and there are 28 organizations from 20 areas on a regional level that are collaborating today. As state-sponsored cyberattacks often come with implications of economic and political signaling, East Asia can continue to deepen the existing "technical only" structure of cyber cooperation to evolve toward a possible "cyber regime complex" (Nye, Jr., 2014) which could work to secure cyberspace through multiple collaborations among governments, the private sector, the technical community, and NGOs in the region.

Furthermore, while the international community is concerned about China's ICT products due to its negative cyber reputation and bad track record, it would be beneficial for regional actors like Taiwan and Japan to shift their focus from developing cyber weapons to developing cybersecurity standards. They can invest in future cybersecurity standards since both countries have accumulated a certain ICT reputation and capabilities. However, the *cooperation* between Taiwan and Japan would not be a kind of military alliance that involves collective defense, as the legal term seems to suggest in the Treaty of Mutual Cooperation and Security between the US and Japan. Instead, it would be cooperation involving the sharing of technological know-how and industrial-oriented development. While the current international structure limits Taiwan's participation in inter-government organizations, collaboration in cybersecurity could be technical and cooperative. It could also circumvent the thorny issue of political recognition making Taiwan a meaningful contributor to international

security. Regional actors like Taiwan and Japan should start to share threat intelligence, develop a technical response, and build common standards against common state-sponsored cyber threats. On November 4, 2019, the US and Taiwan held the first joint cyber exercises to identify their vulnerabilities and enhance their cyber readiness (Hille, 2019), and we are starting to see more joint cyber exercises, training, education, and technical exchanges in the region. Cybersecurity would be better as a competition of cyber talent and not an arms race of cyber arsenals among nations and states.

Conclusion

Cyberspace is a world of our making (Yau, 2018). Sophisticated, tailored malware can now travel across widely interconnected global networks along with possible anonymity and the ability to inject pathologies into any nation. These capabilities can now threaten a wide range of vital elements of modern economic and social contracts that were not historically at risk. In addition, state-sponsored cyberattacks can often be disguised and become a form of "gray zone" operations without affording any legal obligations. Hence, states believe that an effective cyber defense cannot be just reactive and needs to include a proactive element. On the one hand, this does not mean that cyber offence is the solution, as the effectiveness of deterrence should not be exaggerated and the power dynamics in cyberspace are still understudied. On the other hand, although Libicki has pointed out that the best defense in cyberspace is usually a good cyber defense and not necessarily a good cyber offence (Libicki, 2009, p. 176), the involvement of resource-rich actors like China has been eroding the foundation of this argument. While neither argument is perfect and they both have their limitations, this paper argues that a more balanced policy needs to be considered. This is to say that both Taiwan and Japan need defensive cyber capabilities to enhance their defenses in peacetime and an offensive cyber capability to enhance their offensive in wartime. What they should both consider doing more now is establishing closer collaboration in cybersecurity. There is no one-size-fits-all solution, and a state's countermeasures and policy shall depend on the threat posed by the actors they wish to confront.

To conclude, cyberspace is not an alternative to real life but part of it. In the foreseeable future, it is unlikely that cyberwar will simply be a war in cyberspace through cyber means. It will rather be a military conflict in physical domains involving techniques of cyberwarfare. As both Taiwan and Japan are rich in ICT resources, deepening their collaboration in both technical know-how and human resources could offer a better early warning of cyberattacks and further develop a better early warning

for cyber contingency, improve technical know-how on intrusion techniques, and build a positive reputation in the information industry. This is to say that although states cannot effectively deter cyberattacks in peacetime due to the various limitations in cyberspace and may wish to prepare for the unthinkable in wartime regardless of the adverse side effects of their offensive capabilities, they nevertheless must collaborate on cybersecurity, as such cooperation benefits all in both peacetime and wartime.

References

Arquilla, J. (1996). *The advent of netwar.* Santa Monica, CA: RAND Corporation.

Bartos, C. A. (2016). Cyber weapons are not created equal. *US Naval Institute Proceedings*, *142*(6), 30–33.

Berghel, H. (2017). On the problem of (cyber) attribution. *Computer*, *50*(3), 84–89.

Booth, K., & Wheeler, N. (2007). *Security dilemma: Fear, cooperation, and trust in world politics.* Hampshire, UK: Palgrave Macmillan.

Bowcott, O. (2017). Dispute along cold war lines led to collapse of UN cyberwarfare talks. *The Guardian.* Retrieved from https://www.theguardian.com/world/2017/aug/23/un-cyber-warfare-negotiations-collapsed-in-june-it-emerges.

Bright, A. (2007, May 17). Estonia accuses Russia of 'cyberattack'. *The Christian Science Monitor.* Retrieved from https://www.csmonitor.com/2007/0517/p99s01-duts.html.

Broad, W. J., Markoff, J., & Sanger, D. E. (2011, January 15). Stuxnet worm used against Iran was tested in Israel. *The New York Times.* Retrieved from https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Broad, W. J., & Sanger, D. E. (2017, March 14). U.S. strategy to hobble North Korea was hidden in plain sight. *The New York Times.* Retrieved from https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defense.html.

Brodie, B., Dunn, F. S., Wolfers, A., Corbett, P. E., & Fox, W. T. R. (1946). *The absolute weapon: Atomic power and world order*: New York, NY: Harcourt.

Buchanan, B. (2017). *The cybersecurity dilemma: Network intrusions, trust and fear in the international system*. Oxford, UK: Oxford University Press.

Cabinet forms department for cyber security. (2016, August 2). *The China Post.* Retrieved from http://www.chinapost.com.tw/taiwan/national/national-news/2016/08/02/474156/Cabinet-forms.htm.

Chee, F. Y. (2019, November 22). EU countries back tough line on 5G suppliers in potential blow to Huawei. *Reuters.* Retrieved from https://www.reuters.com/article/us-eu-telecoms-idUSKBN1XW276.

Clarke, R. A., & Knake, R. K. (2011). *Cyber war: The next threat to national security and what to do about it*. New York, NY: HarperCollins.

Dai, S. (2019, October 31). What blacklist? China's surveillance industry ignores elephant in the room. *South China Morning Post.* Retrieved from https://www.scmp.com/tech/article/3035563/chinas-surveillance-industry-downplays-us-blacklist-annual-expo-designed.

Executive Yuan. (2016, December 13). *Zhengyuan: Jiji tuidong sinianqi zian qijian jihua, quanmian tisheng tongchuan shiye fanghu nengliang* [政院: 積極推動四年期資安旗艦計畫 全面提升通傳事業防護能量, Press release: Promote 4-year cybersecurity plan to ensure information security capacity]. Retrieved from https://www.ey.gov.tw/Page/9277F759E41CCD91/de4f519d-382f-4207-8459-8b3bf11fda5c.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23–40. doi: 10.1080/00396338.2011.555586.

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, *26*(3), 298–303.

Ghosh, A. (2016, December 19). *Playing the blame game: Breaking down cybersecurity attribution.* Retrieved from https://www.helpnetsecurity.com/2016/12/19/cybersecurity-attribution-blame-game/.

Glaser, C. L. (2011). *Deterrence of cyber attacks and U.S. national security* (Report No. GW-CSPRI-2011-5). The George Washington University Cyber Security Policy and Research Institute. Retrieved https://pdfs.semanticscholar.org/0546/af254548b6636724fb0d2f60122c45fe055f.pdf?_ga=2.168038759.719547047.1591259216-1758763611.1591259216.

Hathaway, O. A., Crootof, R., Levitz, P., & Nix, H. (2012). The law of cyber-attack. *California Law Review*, *100*, 817–886.

Hille, K. (2019, November 4). US and Taiwan host security exercise to boost cyber defence. *Financial Times*. Retrieved from https://www.ft.com/content/7d6c78cc-fec8-11e9-b7bc-f3fa4e77dd47.

Huang, T., & Liu, C.-J. (2017, June 29). *Zitongdianjun zhihuibu biancheng, tongshuai qinlin zhuchi* [資通電軍指揮部編成 統帥親臨主持, The establishment of the Information, Communication, Electronic Warfare Command by the Commander in Chief]. *Youth Daily News.* Retrieved from https://www.ydn.com.tw/News/243100.

Japan slams alleged China-based hackers after cyberattacks on government, firms and colleges. (2018, December 21). *The Japan Times.* Retrieved from https://www.japantimes.co.jp/news/2018/12/21/national/japan-slams-alleged-china-based-hackers-cyberattacks-government-firms-colleges/#.XbeEv-gzZPZ.

Japanese Government. (2018a). *Medium Term Defense Program (FY 2019-FY 2023)*. Tokyo, Japan: Prime Minister of Japan and His Cabinet.

Japanese Government. (2018b). *National Defense Program Guidelines: For FY 2019 and beyond*. Tokyo, Japan: Prime Minister of Japan and His Cabinet.

Jasper, S. (2015). Deterring malicious behavior in cyberspace. *Strategic Studies Quarterly*, *9*(1), 60–85.

Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, *30*(2), 167–214.

Jervis, R., Lebow, R. N., & Stein, J. G. (1989). *Psychology and deterrence.* Baltimore, MD: Johns Hopkins University Press.

Korns, S. W., & Kastenberg, J. E. (2009). Georgia's cyber left hook. *Parameters*, *38*(4), 60–76.

Kurowska, X. (2019). *The politics of cyber norms: Beyond norm construction towards strategic narrative contestation.* Retrieved from European Union Institute for Security Studies website: https://eucyberdirect.eu/content_research/the-politics-of-cyber-norms-beyond-norm-construction-towards-strategic-narrative-contestation/.

Lebow, R. N. (2005). Deterrence: Then and now. *Journal of Strategic Studies*, *28*(5), 765–773.

LegislativeYuan. (2017). *The Legislative Yuan Gazette Vol 106/74.* Taipei, Taiwan: The Legislative Yuan of the Republic of China.

Legislative Yuan. (2019, July 5). *Amendment of National Security Law adds Articles 2-2 and 5-2; and Revises Articles 2-1 and 5-1.* The Gazette of the Office of the President. Retrieved from https://glin.ly.gov.tw/web/nationalLegal.do?isChinese=false&method=legalSummary&id=6438&fromWhere=legalHistory.

Lété, B., & Pernik, P. (2017). *EU-NATO cybersecurity and defense cooperation: From common threats to common solutions.* Retrieved from The German Marshall Fund of the United States website: https://www.gmfus.org/publications/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions.

Lewis, J. A. (2015). *US-Japan cooperation in cybersecurity.* Washington, DC: Center for Strategic & International Studies.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar.* Santa Monica, CA: RAND Corporation.

Libicki, M. C. (2016). Is there a cybersecurity dilemma? *The Cyber Defense Review*, *1*(1), 129–140.

Lieber, K. (2014). The offense-defense balance and cyber warfare. In E. Goldman & J. Arquilla (Eds.), *Cyber analogies* (pp. 96-107). Monterey, CA: Naval Postgraduate School.

Lin, S. (2018, May 12). Info security management act passed. *Taipei Times.* Retrieved from http://www.taipeitimes.com/News/taiwan/archives/2018/05/12/2003692939.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365–404.

Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. *International Security*, *39*(3), 7–47. doi: 10.1162/ISEC_a_00189.

Lutz, D. S. (1983). A counterforce/countervalue scenario — or how much destructive capability is enough? *Journal of Peace Research*, *20*(1), 17–26.

Mazarr, M. J. (2018). *Understanding deterrence*. Santa Monica, CA: RAND Corporation.

Milevski, L. (2011). Stuxnet and strategy: A space operation in cyberspace. *Joint Forces Quarterly*, *63*(4), 64–69.

Ministry of Foreign Affairs (MOFA). (2017, July 3). *Ministry of National Defense launches new Cybersecurity Command.* Retrieved from https://taiwantoday.tw/news.php?unit=2,6,10,15,18&post=117794.

Ministry of National Defense (MND). (2017). *2017 Quadrennial Defense Review: Republic of China.* Taipei, Taiwan: MND.

MND. (2019). *2019 National Defense Report, Republic of China.* Taipei, Taiwan: MND.

Morgan, P. M. (2003). *Deterrence now.* Cambridge, UK: Cambridge University Press.

National Center of Incident Readiness and Strategy for Cybersecurity. (2018). *Cybersecurity Strategy 2018.* Tokyo, Japan: NISC.

Nye, Jr., J. S. (2014). *The regime complex for managing global cyber activities* (Global Commission on Internet Governance Paper Series No. 1). Retrieved from https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. *International Security*, *41*(3), 44–71.

Office of the Director of National Intelligence. (2018). *A guide to cyber attribution.* Washington, DC: ODNI.

Office of the President. (2018, September 14). *Announce "National Cybersecurity Strategy Report": Cybersecurity as National Security.* Retrieved from https://www.president.gov.tw/Page/317/969/%E5%9C%8B%E5%AE%B6%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E6%88%B0%E7%95%A5%E5%A0%B1%E5%91%8A-%E8%B3%87%E5%AE%89%E5%8D%B3%E5%9C%8B%E5%AE%89-.

Prime Minister's Office. (2013). *National Security Strategy of Japan.* Tokyo, Japan: Prime Minister of Japan and His Cabinet.

Rid, T. (2013). *Cyber war will not take place.* Oxford, UK: Oxford University Press.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37.

Rosenzweig, P., Bucci, S. P., & Inserra, D. (2017, May 5). *Next steps for US cybersecurity in the Trump Administration: Active cyber defense* (Backgrounder No. 3188). Retrieved from http://report.heritage.org/bg3188.

Schmitt, M. N. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations.* Cambridge, UK: Cambridge University Press.

Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security*, *41*(3), 72–109. doi: 10.1162/ISEC_a_00267.

Snyder, G. H. (1959). *Deterrence by denial and punishment.* Princeton, NJ: Woodrow Wilson School of Public and International Affairs, Center of International Studies, Princeton University.

Snyder, J. L. (1984). *The ideology of the offensive: Military decision making and the disasters of 1914.* Ithaca, NY: Cornell University Press.

Stoddart, K. (2016). Live free or die hard: U.S.-UK cybersecurity policies. *Political Science Quarterly*, *131*(4), 803–842.

UN General Assembly. (2015). *Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security.* Retrieved from CCDCOE website: https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf.

UN General Assembly. (2019). *Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security.* Retrieved from United Nations website: https://undocs.org/A/AC.290/2019/1.

US DoD. (2015). *The DoD cyber strategy.* Washington, DC: U.S. Department of Defense.

Walt, S. M. (1998, Spring). International relations: One world, many theories. *Foreign Policy*, *110*, 29–46.

Yau, H.-M. (2015). *Handle with care: The pandora's box of cyber attacks.* Retrieved from http://thinking-taiwan.com/thinking-taiwan.com/handle-with-care-pandoras-box-cyber-attacks/index.html.

Yau, H.-M. (2018). Explaining Taiwan's cybersecurity policy prior to 2016: Effects of norms and identities. *Issues & Studies*, *54*(2), 1–30. doi: 10.1142/s1013251118500042.

Yau, H.-M. (2019a). A critical strategy for Taiwan's cybersecurity: A perspective from critical security studies. *Journal of Cyber Policy*, *4*(1), 35–55.

Yau, H.-M. (2019b). An assessment of cyberpower within the triangular relations of Taiwan-US-China and its implications. *International Journal of Taiwan Studies*, *2*(2), 264–291.

LIBRARY RECOMMENDATION FORM

Route via interdepartmental mail

Dear Librarian / Library Acquisition Committee

I would like to recommend the **Issues and Studies (IS)** for the library. Please include it in your next serials review meeting with my recommendation.

If you require further sample copies, please contact your nearest World Scientific Office. You can also obtain further information at www.worldscinet.com.

NAME _____

POSITION _____

DEPARTMENT _____

I recommend the journal for the following reasons:
(plesase tick)

- ❑ REFERENCE: I will need to refer to this journal frequently for my work
- ❑ STUDENT REFERRAL: I will be referring my students to this journal regularly to assist their studies
- ❑ I have other reasons for recommending this journal which are as follows:
- ❑ BENEFIT FOR LIBRARY: This journal will complement the library's collection and I will regularly recommend articles to my colleagues / students
- ❑ OWN AFFILIATION: I am a member of the journal's sponsoring society / editorial team. I therefore strongly support the journal

_____

_____

_____

ORDER FORM

Subscribe now through our journal website: **www.worldscinet.com** or fax the completed order form to **(65) 6467 7667**

❒ Please send me a complimentary copy of the **Issues and Studies (IS)**
❒ Please process my subscription:

ISSN: 1013-2511 **Vol. 56 • 4 Issues • 2020**

Institutions/Libraries (Print* + Electronic)	❒ US$366	❒ £293	❒ S$497
Institutions/Libraries (Electronic Only)	❒ US$333	❒ £266	❒ S$452
*Please add postage	US$40	£31	S$53

- Customers from Asia Pacific and Australasia (except Hong Kong and China), please pay in Singapore Dollars (**S$**).
- Customers from Europe, please pay in GBP (**£**).
- Customers from the rest of the world (including Hong Kong and China), please pay in **US$**.

Please enclose your personal cheque or details of your credit card for individual journal subscriptions.

Name: _____ Email: _____

Organization: _____ Department: _____

Address: _____

City: _____ State: _____ Zip: _____ Country: _____

METHODS OF PAYMENT :

❒ Cheque/Bank draft enclosed for the amount of US$/£/S$ _____

- For cheque payment, please make cheque payable to "**World Scientific Publishing Co. Pte. Ltd.**"

Charge my ❒ VISA ❒ MC ❒ Amex

Card No: | | | | | | | | | | | | | | | | Expiry Date: | | | | | | |

Tel: _____ Signature: _____

❒ Bill my company/institution: _____ (Please attach purchase order)

Credit Card Authorisation

By completing this Credit Card Authorisation Form, I am authorizing and giving consent to World Scientific Group of Companies to
1) debit my credit card account for one-time payment for the purchase of the product stated above;
2) retain my credit card information for a period of one year for audit purposes.

Back volume prices are available upon request

Affix
Stamp
here

World Scientific Publishing Co. Pte. Ltd.
Farrer Road, P O Box 128
Singapore 912805
Republic of Singapore

Issues & Studies

A Social Science Quarterly on China, Taiwan, and East Asian Affairs

AIMS AND SCOPE

Issues & Studies (ISSN 1013-2511) is published quarterly by the Institute of International Relations, National Chengchi University, Taipei. *Issues & Studies* is an internationally peer-reviewed journal dedicated to publishing quality social science research on issues — mainly of a political nature — related to the domestic and international affairs of contemporary China, Taiwan, and East Asia, as well as other closely related topics. The editors particularly welcome manuscripts related to China and Taiwan.

SUBMISSION OF MANUSCRIPTS

Submitted manuscripts should meet the guidelines spelled out in the "Information for Authors" that is available on our website: http://issues.nccu.edu.tw. Any questions regarding submissions or general policy should be addressed to <issues@nccu.edu.tw>.

Editorial Office:

Issues & Studies
Institute of International Relations
National Chengchi University
No.64, Wanshou Road, Wenshan District 116, Taipei City, Taiwan (ROC)
Tel: 886-2-8237-7377
Fax: 886-2-2939-7352
E-mail: issues@nccu.edu.tw
Website: http://issues.nccu.edu.tw

INDEXES AND ABSTRACTS

Articles in *Issues & Studies* are indexed by *Scopus*, *Google Scholar*, *EBSCO*, *ProQuest*, *Current Contents*, *Research Alert* (Institute for Scientific Information, Philadelphia), *ABC POL SCI* (ABC-Clio, Inc., Santa Barbara, California), and *IBZ* (International Bibliography of Periodical Literature in the Humanities and Social Sciences) and *IBR* (International Bibliography of Book Reviews of Scholarly Literature in the Humanities and Social Sciences) (Osnabrueck, Germany); abstracted by the *International Political Science Abstracts* (*Documentation Politique Internationale*, Paris) and *International Development Abstracts* (Oxford, England); and abstracted and indexed by the *International Bibliography of the Social Sciences* (London) and *Sociological Abstracts* (San Diego, California).

Issues & Studies

A Social Science Quarterly on China, Taiwan, and East Asian Affairs

Vol. 56, No. 3 **September 2020**

CONTENTS

Special Issue: Multidimensional Security Issues in Asia
Guest Editor: Chyungly Lee

ISSN: 1013-2511 MCI (P) 025/08/2020