MIDDLE POWER CYBERSECURITY IN THE INDO-PACIFIC: AN ANALYSIS THROUGH THE LENS OF NEO-MIDDLE POWER DIPLOMACY

Thomas J. Murphy, *International Christian University,*
Japan

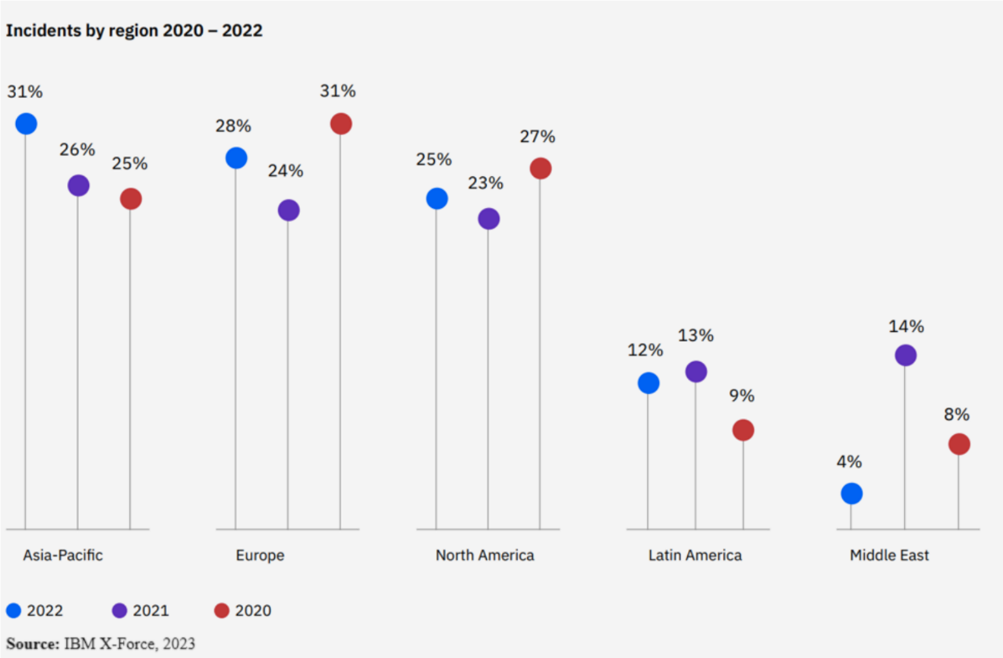
Stephen R. Nagy, Department of Politics and International Studies,
International Christian University,
Japan

Abstract

As technology has advanced and our world has become increasingly interconnected, cyberspace has become a key battlefield in great-power competition. The Indo-Pacific has found itself vulnerable in this new reality — the paucity of institutions, heterogeneity in levels of development, and the region being the primary zone of US-China competition fueling these vulnerabilities. Cyberspace provides a multitude of security threats posed by states, non-state actors and state-sponsored actors. Despite this, cybersecurity takes a backseat to other security issues despite its critical importance. Using the concept of neo-middle power diplomacy, this paper examines why the limited cybersecurity cooperation among middle powers in the Indo-Pacific has taken the shape it has. This paper finds that the two most promising areas of cooperation for middle powers are through confidence-building measures and capacity-building measures. Through actively pursuing these two measures, middle powers can become more effective, capable, and autonomous stakeholders within the Indo-Pacific.

COVID-19, the war in Ukraine, and the economic ascent of China and the resulting rising tensions between China and the United States have contributed to the deterioration of the post-Cold War international order. The cyber domain has not found itself stagnant or immune considering these developments. In tandem with these global events, we have witnessed a record high in the number of cyber-attacks reported around the globe targeting both state and non-state actors (Callanan et al., 2022). Data provided by the Harvard Business Review notes that data breaches in both private and public sectors continue to increase on a year-by-year basis, with a 20% increase in 2023 resulting in 360 million people falling victim to these attacks (Madnick, 2024).

Figure 1
Incidents by region 2020-2022



Source: IBM X-Force, 2023

Source: IBM, 2023

Additional data suggests that since 2020, the Indo-Pacific has been the most targeted region in the world. IBM's X-Force annual report shows that Asia was the most attacked geographical location in the world in 2021 — over 26% of global attacks targeting the region — with an estimated 80% of organizations in the region having been hit by ransomware attacks (IBM, 2023; Kimhy & Tribbey, 2022). Cyber cooperation in the region has remained limited, despite hosting several of the world's foremost cyber powers, such as the United States, China, South Korea, Australia, and middle powers capable of coalition building (Kim, 2022; Voo et al., 2022). Most notably, there has yet to be developed a multilateral framework regarding cyber conflict as it relates to regional security (Richey, 2022). Due to this rising tide of cyber threats, middle powers and the role they play in shaping regional security becomes increasingly crucial.

What are middle power states and how do they act diplomatically to secure their interests? Modern conceptions of middle power have been built on the blocks laid by Chapnick and others, such as Cooper, Higgott, and Nossal following the Cold-War period. Often, this conceptualization consists of adapting Chapnick's three models of middle powers and either redefining the existing models or adding new ones to better reflect their contemporary realities. The three models of middle powers put forth by Chapnick are the functional model, the behavioral model, and the hierarchical model (Chapnick, 1999).

The functional model of middle powers revolves around the capabilities and functions of a state. This model weighs and evaluates states by the influence they can exert in international affairs in specific situations, as well as by their status which fluctuates according to a state's level of political and economic strength relative to the great powers of the time. The hierarchical model views middle powers under the lens of an international hierarchy of states with three differing strata or classes, defined by a state's objective capability, asserted position, and recognized status within a hierarchical, stratified international system (Dewitt & Kirton, 1983). This hierarchical model can best be understood in the Indo-Pacific through a viewing of the Lowy Institute's Asia Power Index. According to this index, there are three different strata of states in line with the hierarchical, or empirical model, namely: super powers; middle powers; and minor powers (Lowy, 2023). The middle powers within the region that the Lowy Institute identifies according to their methodologies accounting for capabilities and influence are in descending order of power: Japan; India; Russia; Australia; South Korea; Singapore; Indonesia; Thailand; Malaysia; Vietnam; New Zealand; Taiwan; Pakistan; Philippines and North Korea (Lowy, 2023). As explained by Nagy and Ping in their Australian Institute for International Affairs essay, this empirical model furthers the hierarchical model by not only comparing the middle powers to super and minor powers, but amongst themselves as well.

However, it says nothing about their behavior, the nature of diplomacy, as well as the convergences and divergences amongst them (Nagy & Ping, 2023).

The behavioral model is centered on the idea that middle powers are defined through their behavior on the international stage and how they act in ways that either we assume they should act or in ways we prescribe to middle powers. This is a slightly outdated view, predicated on the notion that middle powers behave in ways aligned with the existing liberal international order — championing human rights, human security, and an overall morally centered foreign policy.

Jonathan Ping's hybridization theory is perhaps the most significant evolution in middle power theory in recent times. Ping asserts that middle powers are intrinsically hybridizers and that middle power statecraft and the perceived powers of middle powers are fundamentally different in comparison to great and small powers (Ping, 2017). This theory, unlike its predecessors, accounts for the diverse range and behavior of middle powers who are otherwise united under this label, from Canada and Australia to Indonesia and Malaysia, by taking into account the hybridisation of their respective middle power statecraft and perceived power. What this means is that states will hybridize external sources for the purpose of creating new and unique forms of statecraft and perceived power in order to compete successfully against their neighboring middle powers, lest they become vulnerable and potentially overtaken (Ping, 2017). Unlike Chapnick and others who put forth a functional model of middle powers, Ping contests that their power comes from a variety of factors that include strategic territory, military and economic resources, ideology, and levels of economic development. Additionally, Ping asserts that you cannot define a middle power according to a formula or model, rather, identification is based most strongly on the ability of the definer (Ping, 2017).

This evolution in the theorization and definitions of middle powers reaches its culmination for us in the form of neo-middle power diplomacy. Providing for us both a unique and practical lens to understanding the capabilities of middle powers in coalition building and cooperation, and key to discerning how middle powers understand the domain of cyberspace and its associated threats to national security, Stephen Nagy defines neo-middle power diplomacy as:

> Proactive foreign policy by middle powers that actively aims to shape regional order through aligning collective capabilities and capacities. What distinguishes neo-middle power diplomacy from so-called traditional middle power diplomacy is that neo-middle power diplomacy moves beyond the focus of buttressing existing international institutions and focusing on normative or issue-based advocacy such as human security, human rights or the abolition of land mines, to contributing to regional/global public goods through cooperation, and at times in opposition to, the middle powers' traditional partner, the US. Areas of cooperation [may include] … maritime security, surveillance, HADR, joint transits, amongst others (Nagy, 2020).

As Domingo notes, cyber capabilities are critical tools for those who call the Indo-Pacific home, primarily due to the continuing heightening of the geopolitical rivalry between the United States, China, and their allied countries in the region (Domingo, 2022). This geopolitical rivalry between the two "superpowers" to expand their reach and influence in the Indo-Pacific is, as Domingo notes, a key factor in contributing to the growing importance of cyber capabilities — in addition to the acquisition of cyber capabilities to further domestic goals at home, such as the consolidation of domestic political systems and political repression by authoritarian states. According to Belfer's National Cyber Power Index, cyber capabilities can be measured in the context of seven national objectives: financial; surveillance; intelligence; commerce; defense; information control; destructive; and norms (Voo et al., 2022). Countries across the globe find themselves having greater cyber capabilities in regard to the fulfillment of specific national objectives compared to others. Examples in the region include the DPRK and their capability in amassing and protecting wealth for the financial objective; China and Vietnam's surveillance capabilities; as well as Singapore's capabilities in intelligence collection (Voo et al, 2022). However, unlike the great powers of the United States and China, the majority of the countries that call the Indo-Pacific home are small and middle powers, states without the resources and capabilities necessary to shape cyberspace and discussions on cybersecurity by themselves. Additionally, the Indo-Pacific and the countries and multilateral groupings within the region are not homogeneous. Rather, they are incredibly diverse. A common problem and misunderstanding when discussing small and middle powers in the Indo-Pacific — states other than the United States and China — is the tendency to group them into factions, a paradigm of West versus non-West, liberal democracies versus authoritarian dictatorships, those aligned with the United States and those aligned with China. One needs look no further than the states that make up ASEAN to see the insufficiencies in such an outlook. Contained within ASEAN are a multitude of soft authoritarian states, states assumed to be client states, and even a state undergoing a coup. Looking past the two great powers in the region, the Indo-Pacific is neither homogeneous nor dichotomous.

Despite this, a discussion on cyberspace, cybersecurity, and the region as a whole cannot take place without the inclusion of these incredibly diverse middle powers and their role within the Indo-Pacific in shaping the discussion on cybersecurity. These small and middle powers find themselves locked in a battleground between the United States and China, with both great powers vying for their support in shaping an Indo-Pacific that is in line with their own respective visions, often to the disinterest of the states in the region who wish not to get caught up in this great power rivalry, seeking to balance and hedge against them instead (Nagy, 2022).

As such, in this paper, we seek to analyze the capabilities of middle powers in cyberspace through the lens of neo-middle power diplomacy, examining the multitude of threats these states face from cyberspace, and how these states can cooperate within the Indo-Pacific with the aim of securing a safe and prosperous region for all. As part of this, this paper seeks to examine the research puzzle of why middle powers in the Indo-Pacific engage in both confidence building measures and capacity building measures through the lens of neo-middle power diplomacy in order to understand how middle powers in the region are engaging in cooperation.

Cyberspace and Middle Powers

Cyber as a concept is one that is complex, containing multiple sub-concepts and sub-definitions. Ottis & Lorents propose their own definition of cyberspace, unique in its formulation through the inclusion of time-dependence. Citing Strate's concept of cyberspacetime, defined as "the totality of events involving relationships between humans and computers, between humans through computers, and between computers themselves." (Strate, 1999) Ottis & Lorents identify that this definition is lacking as it fails to consider the inherent dynamic nature of cyberspace, and instead holds cyberspace as a static setting in its encompassing of the collective nature of cyberspace in its entirety (Ottis & Lorents, 2010).Viewing existing definitions of cyberspace as too vague or even incomplete, as well as not considering the dynamic nature of cyberspace, they propose a definition of cyberspace that states "cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems" (Ottis & Lorents, 2010). Sharing in this definition with Lehto's later definition is the inclusion of human users. This inclusion is crucial for Ottis & Lorents, asserting that as a human created space, it is one that becomes stagnant and further ceases to exist without human users. Yet for them, it is the dynamic nature of cyberspace that is the key in their formulation of cyberspace — asserting that dramatic changes can take place in an extremely short time in cyberspace in comparison to other time-dependent systems As such, they define time-dependence as "the change in the structure and content of cyberspace over time" (Ottis & Lorents, 2010). This additional concept of time-dependence becomes increasingly important as technology continues to develop and we are introduced to augmented realities, such as the metaverse.

Following this, cybersecurity, at its core, is a very broad term with crossover in a variety of different fields and disciplines with cyberspace at its core. Wanting to utilize a definition that incorporates all of the above aspects and embodying a multisectoral approach, for the remainder of this paper we shall utilize the definition of cybersecurity put forth by Fang which is as follows:

> Cyberspace security involves security issues that exist in electromagnetic equipments, information communication systems, operating data and system applications in cyberspace. It must not only protect the ICT system—including the Internet, various telecommunication networks and communication systems, various communication systems and radio and television networks, various computer systems, and embedded processors and controllers among various key industrial facilities—and data carried by it from being attacked, but also prevent against and cope with risks concerning political security, national defense security, economic security, cultural security, social security and the like, which result from the use or abuse of the ICT system. Dealing with those risks needs comprehensive means such as law, management, technology and self-discipline, so as to guarantee confidentiality, identifiability (including

> integrity, authenticity, and non-repudiation), availability and control of the ICT system and the data carried by it (Fang, 2018).

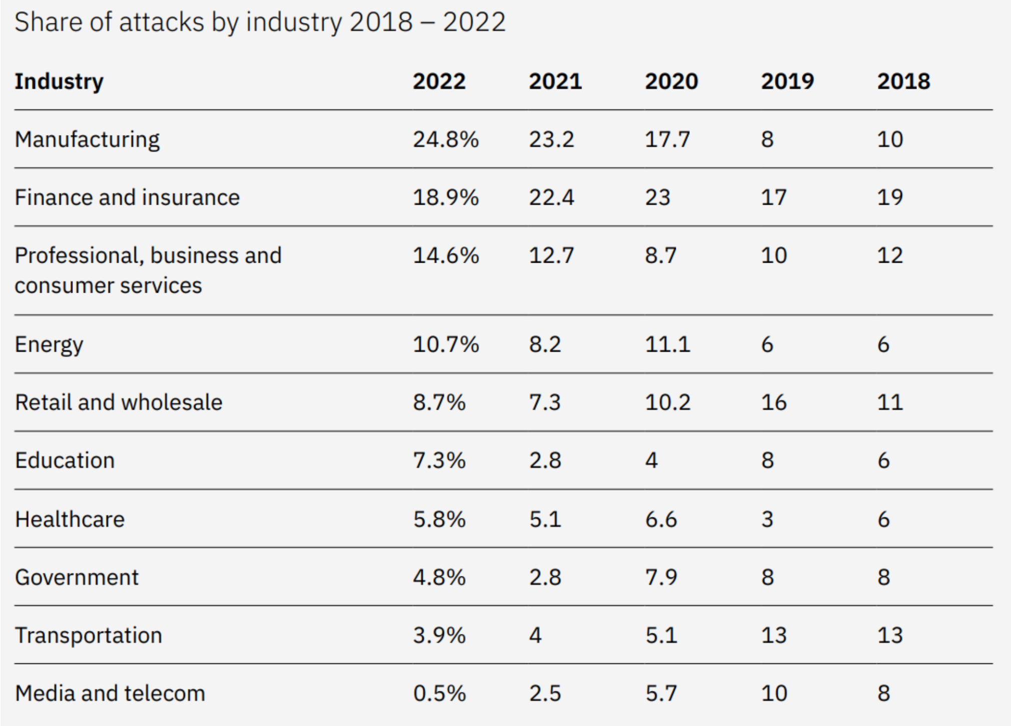
Capabilities of Middle Powers

As Domingo notes, to effectively explore the utility of cyber capabilities and how they can affect our reality and policy choices outside of cyberspace, it is essential to assess the cyber capabilities of states under the lens of foreign policy and how they can serve as foreign policy instruments to pursue national interests (Domingo, 2022). Yet, what are the capabilities and intentions of the middle powers in the Indo-Pacific? As previously mentioned, the region is far from homogeneous, and as such the capabilities and intentions of middle powers that call the region home can differ drastically. However, by and large, Kim notes that middle powers seek to exercise, gain, and maintain collective power through coalition building (Kim, 2014). Here, he notes the role of South Korea in performing the role of a middle power through the theory of network diplomacy to advocate for middle powers to attract as many like-minded countries as possible to attain their goals in cyberspace, becoming a broker in the sector of cybersecurity (Kim, 2014). As Richey has established, there has yet to be developed a multilateral framework regarding cyber conflict as it relates to national security despite the Indo-Pacific and the globe at large facing national security threats from the increasing sophistication of cyber capabilities and cyber conflict (Richey, 2022). However, the role of middle powers as coalition builders, in line with neo-middle power diplomacy, pushes us beyond the focus of buttressing existing international institutions, to instead contributing to regional/global public goods through cooperation. Most of the time, this role finds itself aligned with the United States and the international liberal order, yet this is not a requisite alignment.

Middle powers are key to the regional discussion of cybersecurity and for any future of coalition building and cooperation. The Belfort Center for Science and International Affairs at the Harvard Kennedy School in their 2022 National Cyberpower Index has ranked three middle powers in the Indo-Pacific as members of the top 10 of international cyberpowers, these middle powers being Australia, The Republic of Korea, and Vietnam (Voo et al, 2022). Additionally, a multitude of countries that define themselves as Indo-Pacific nations find themselves within the top 10 in certain areas of cybersecurity. However, how is cyber power defined? Nye defines cyberpower as “a set of resources that relate to the creating, control and communication of electronic and computer-based information — infrastructure, networks, software, human skills” and refers, behaviourally, to ‘the ability to obtain preferred outcomes through the use of the electronically interconnected information resources of the cyber domain” (Nye, 2010). Following this, scholars such as Dunn Cavelty remark that there is a widespread agreement in the relevant literature that cyberpower as a concept can be utilized to produce outcomes preferable to an actor's national interests as well as effects created through cyber instruments that lay outside the cyber domain (Dunn Cavelty, 2018). There is widespread agreement in the literature that cyberpower can be used to produce preferred outcomes within cyberspace or it can be linked to effects created through cyber-instruments outside cyberspace (Dunn Cavelty, 2018). The region finds itself with a relatively high level of competence and expertise in cybersecurity. However, the key to this understanding of middle powers and their cyber capabilities is that their cyber power is not primarily military leaning in scope. Rather, they are more focused on economy, information, and development. As seen from IBM’s Security X-Force Threat Intelligence Index 2023 report, the manufacturing, finance, and professional services industries are the most targeted by cyberattacks (IBM, 2023). The Indo-Pacific finds itself uniquely affected, with the manufacturing and development industry accounting for 48% of all cases in the region. Another key feature of the Indo-Pacific region is the vulnerability of its governments, with government entities within the Indo-Pacific making up 50% of all government targeted cyber-attacks in 2022 (IBM, 2023).

Figure 2

Share of attacks by industry 2018-2022



Share of attacks by industry 2018 – 2022

Industry	2022	2021	2020	2019	2018
Manufacturing	24.8%	23.2	17.7	8	10
Finance and insurance	18.9%	22.4	23	17	19
Professional, business and consumer services	14.6%	12.7	8.7	10	12
Energy	10.7%	8.2	11.1	6	6
Retail and wholesale	8.7%	7.3	10.2	16	11
Education	7.3%	2.8	4	8	6
Healthcare	5.8%	5.1	6.6	3	6
Government	4.8%	2.8	7.9	8	8
Transportation	3.9%	4	5.1	13	13
Media and telecom	0.5%	2.5	5.7	10	8

Source: IBM X-Force, 2023

Despite these multi-sectoral threats, it is clearly a response to military buildup and rising tensions that have spurred middle powers in the Indo-Pacific to advance their cyber capabilities. All of the aforementioned background on the region, as well as the acquisition and proliferation of conventional military arms, has inspired an equal level of acquisition and proliferation of cyber capabilities in the Indo-Pacific to either protect or advance the national and foreign policy interests of relevant middle powers in the region. Spanning geographically from the Pacific Ocean to the Western Indian Ocean, the Indo-Pacific is unique in this aspect for a multitude of reasons, but perhaps the most significant is the prevalence of enduring rivalries and conflicts in the region by neighboring countries. South Korea and North Korea, India and Pakistan, Taiwan and China, all of these conflicts and rivalries are relatively localized, however, as technological advances within these respective countries occur, the conflict spills over into cyberspace. Valeriano and Maness note how South Korea has been compelled to develop its cyber capabilities at a rapid rate to protect its critical infrastructure against targeted cyber-attacks from North Korea (Valeriano and Maness, 2015) and China, (Ernst & Lee, 2021), but also from state-sponsored groups that launch attaches from these territories (Ernst & Lee, 2021). Additionally, conflicts between India and Pakistan have found their way into the cyber domain, usually coinciding in the context of tit-for-tat moves or on important dates such as Independence Day (Shad, 2019) and the role of Taiwan in the semiconductor industry makes their cyber defense synonymous with national defense. Betz adds that national defense has served as a strong motivator for weaker states, such as middle and small powers, to develop their own cyber capabilities as military operations that fall outside of the scope of war, such as peace enforcement and humanitarian assistance also require advanced capabilities that are reliant on information and communication technologies (Betz, 2009). Domingo remarks that "cyber capabilities have become a fundamental prerequisite for states deploying twenty-first-century military capabilities" (Domingo, 2022).

However, one of the true values of cyber capabilities for middle powers is their use in protecting non-government interests in cyberspace, including private companies and civil society, made into an even more pressing area of potential cooperation among middle powers due to the sheer resource gap between them and great powers (Domingo, 2022). These sectors are of the utmost priority due to their contributions to the development of capacity, resources, and norms necessary for states to manage the power imbalance currently inherent in the Indo-Pacific as well as the insecurity of the cyber domain in the region (Harknett and Stever, 2009; DeNardis, 2014; Hoffman and Levite, 2017; Domingo, 2022). Further, Domingo notes that middle powers like Australia, South Korea, and Japan do not have the same level of capabilities and resources that great powers such as the United States and China do, yet they are equally as motivated to develop their own cyber capabilities to supplement their conventional military/self-defense weapons (Domingo, 2022). Additionally, most middle powers in the region, including relatively cyber-strong middle powers such as Malaysia, (Voo et al., 2022) have developed their own cyber capabilities in a defensive direction with the protection of non-military interests at the forefront of their mind, including the defense of the private sector, trade, and diplomatic channels with neighboring states in the Indo-Pacific (Voo et al., 2022).

Taken together as a whole, middle powers in the Indo-Pacific view the acquisition and development of cyber capabilities as a key priority to protect their national interests, defend their governmental and non-governmental interests — such as the private sector — and navigate the ever-developing geopolitical rivalry between the United States in China, lest they be caught in the crossfire. This is the direction the development of their cyber capabilities is taking, and it is where they currently lie. Where then can any potential cooperation between middle powers in the Indo-Pacific take place regarding cyberspace? This paper highlights two primary areas that cybersecurity cooperation can take place between middle powers: confidence-building measures and capacity-building measures, in line with the neo-middle power diplomacy argued by Nagy.

Confidence-Building Measures

Ziolkowski defines confidence-building measures (CBMs) as "an instrument of international politics, negotiated by and applied between states. CBMs aim to prevent the outbreak of an (international) armed conflict by miscalculation or misperception of the risk and by the consequent inappropriate escalation of a crisis situation, by establishing practical measures and processes of (preventive) crisis management between States" (Ziolkowski, 2013). Additionally, confidence-building measures in general contain aspects of transparency, cooperation, and stability. In defining these three aspects, Ziolkowski states that transparency measures serve the purpose of fostering a better mutual understanding between states of national military capabilities and their military activities, cooperation measures refer to any collaborative effort between states, including the enhancing of documents, joint military exercises, exchange of observers, visits between delegations and developing a common understanding between participating countries of relevant key terms and definitions, and stability measures deal with the the fostering of predictable military activities and a stabilization on the military balance between participating countries in order to better effectively collaborate (Ziolkowski, 2013).

As can be seen, confidence-building measures are traditionally linked to the military domain and in building confidence, specifically in regard to the militaries of participating nations. As cybersecurity has risen not only as a military issue, but a hybrid threat, cyber confidence-building measures have emerged as their own distinct tool. This can be further correlated to the historical development of confidence-building measures as a response to technological innovation and geopolitical dynamics. Borghard & Lonergan remark that this took place historically for states to either form their own confidence-building measures or to go in another direction and to create arms control regimes with the idea of institutionalizing constraints on new and developing offensive military technology and to guard against inadvertent conflict and escalation (Borghard & Lonergan, 2018). They note that at their core, confidence-building measures provide reassurance through four mechanisms: the increasing of transparency of military actions; self-imposed limits on security activities; enabling lines of communication between adversaries; and conveying intent behind a state's security policies and actions. Borghard & Lonergan note that although confidence-building measures on their own cannot serve the role or even replace national technical means of intelligence, they serve to supplement it by enabling a fuller picture of the relevant parties to the confidence-building measures and to the significance of a military policy or action than otherwise would have been available (Ziolkowski, 2018).

Confidence-building measures for cyberspace can be potentially just as effective as their counterparts in other domains. One such area that would be particularly effective in regard to cybersecurity is that of political commitments and alignments. Ziolkowski argues that confidence-building measures for cyberspace can serve as a powerful tool for political declarations by states that are significant for the progressive development of international law (Ziolkowski, 2013). Ziolkowski puts forth a number of suitable measures for confidence building measures in cyberspace that can serve as a suitable model, drawing from the Consolidated List of Confidence and Security Building Measures put forward by the Organisation of American States Permanent Council. Translated to cyberspace and cybersecurity, these confidence building measures transform to: “exchange of information on the organization, structure, size, and composition of computer network operations (CNO) units, advance notice of live hacking exercises by CNO units, conduct of joint training and exercises between CNO units, and visits of CNO units and their computer laboratories.” Additional measures included on the OAS list include: “exchange of defense policy and doctrine papers, establishment of national points of contact regarding critical infrastructure protection, exchange information on scientific research, and exchange of contracts between students, academics, and experts in defense and security studies” (Ziolkowski, 2013). Measures such as these have already been undertaken by middle powers in the region to enormous success. One need not look further than ASEAN to see this. Under the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies, 7 confidence-building measures were adopted over 10 meetings from intersessional years 2018 to 2021. (ASEAN, 2022)

As noted by the Global Forum on Cyber Expertise, the UNGGE in its 2015 report provided the groundwork for increased involvement of regional organizations when it comes to implementing confidence-building measures in cyberspace (GFCE, 2020). Due to their common historical and cultural ties, regional organizations are uniquely equipped to develop and to effectively implement these confidence-building measures as opposed to international bodies. Due to this, it is easier for them to focus on the practical application of confidence-building measures as well as implementing effective ones that will work specifically for them, serving to develop the groundwork necessary for enhanced communication, transparency, and collaboration in cyberspace (GFCE, 2020). This is reflected in the efficacy of ASEAN's confidence-building measures in addressing the primary goals of their measures.

Why confidence-building measures are so key for middle powers in engaging in cybersecurity cooperation is due to the vulnerability of information shared in cyberspace. As discussed in a Chatham House seminar hosted by the Yokosuka Council on Asia Pacific Studies on the topic of creating a more inclusive AUKUS, reservations in key areas such as information sharing exist and are a major block toward a middle power's potential inclusion in the minilateral due to concerns over their defense and information security capabilities (YCAPS, 2023). These concerns can be alleviated through the sharing of cyber confidence-building measures among states, enabling middle powers to bolt on to the existing structures of allies and regional partners, as was the case with Canada and its bolting onto the QUADs Sea Dragon 21 exercises in 2021 (Paskal, 2021; Nagy, 2022). Additionally, the very nature of cyberspace capabilities may make any potential cooperation or bolting inherently different, based on the differences between offensive, defensive, and information-based capabilities, further necessitating the need for confidence building measures among potential allies. Through the utilization of cyber confidence-building measures, talks of a QUAD plus or an AUKUS plus may potentially be realized (Nagy, 2021).

In addition to confidence-building measures, another type of CBM in which cybersecurity cooperation can take place between middle powers is *capacity-building measures*. As opposed to confidence-building measures, capability-building measures are more widespread and thought of in foreign policy discussions. The reasons for these key contributions to nations' cyber-security agendas are plentiful. Capacity-building measures are closely linked to foreign direct investment and as such, are a much more popular tool to gain influence in another state, and the benefits of such investment are often tangible, either in the alignment of the recipient countries' interests with that of the donor state, or through increased productivity in the areas of trade, transportation, or communication. This is double so in the Indo-Pacific region, where there is a stark divide between developed and developing states, as well as multiple hands in the donor pot, from developed middle powers, great powers, minilateral and multilateral regional bodies, and regional banks.

Homburger, in their tracking of the evolving definitions of capacity building, notes that cybersecurity capacity building is often defined in the relevant literature as a form of support provided to developing, or recipient countries to increase access to and benefit from cyberspace from a donor country (Homburger, 2019). These academic definitions stemming from the literature, Homburger remarks, find their basis in the traditional concept of capacity building, which focuses primarily on economic development as the aim of activities. As such, these capacity-building measures have a heavy emphasis on the relation between the involved states, oftentimes taking the form of a donor-recipient relationship as well as a developed-developing dynamic. With this relationship between donor and recipient in mind, Homburger notes that other authors define cybersecurity capacity building as "a way to empower individuals, communities and governments to achieve their developmental goals by reducing digital security risks stemming from access and use of information and communication technologies." Not satisfied with this definition, Homburger provides for us a more rounded definition, defining cybersecurity capacity building as "support and assistance aiming at empowering individuals, communities and governments to reduce risks stemming from access and use of information and communication technologies." (Homburger, 2019)
Japan has been focused much more in line with their own capabilities as a middle power toward cyber capacity-building measures since as early on as 2013, yet in the role of a regional leader despite their middle power status. Not as single-

mindedly concerned with shaping the debate on global norms for cyberspace as China is — although still greatly interested — Japan's cyber capacity-building measures have mainly served to push forward their national interests in the shape of of human resource development, sharing of best practices, cross-border cooperation, and intelligence sharing through training, starting with the J-Initiative for Cybersecurity established in 2013 (Malachinski, 2023). As a result, the three core objectives of Japan's cyber diplomacy are "(1) the promotion of the rule of law in cyberspace; (2) the development of confidence-building measures; and (3) cooperation in capacity building" (Vosse, 2022). Adding onto these three core objectives, Bimantara puts forth three material drivers for Japan's assistance. (1) prestige; in their desired role as a regional leader on cybersecurity issues, undertaking regional capacity-building measures aids Japan in building an image in which recipient countries will perceive them as a role model in capacity-building measures and one that should be emulated in the future; (2) capacity-building measures are a boon when it comes to "politico-diplomatic" concerns that further aid their own interests; and (3) through enacting capacity-building measures in developing countries, they can at the same time promote economic development, creating an additional and more advanced market for them to engage with (Bimantara, 2022). Focusing on their cybersecurity strategy, Vosse outlines the importance of cyber capacity-building in the Japanese context by framing it alongside their 2018 cybersecurity strategy document and their many active cyber capacity-building measures currently being undertaken in the region. These include the establishment and funding of the Japan was central in setting up and funding the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Bangkok in September 2018 as well as the Japan-ASEAN Information Security Policy Meeting. Vosse remarks that Japan's cyber capacity-building measures serve to advance their national interests in two main ways: firstly, through the strengthening of a regional understanding, awareness and support for an open and free internet and the rule of law in cyberspace through the improvement of the skills of security-related agencies in the 10 ASEAN countries, and secondly, in the establishment of a standardized Incident Reporting Framework across the Indo-Pacific by founding an ASEAN-CERT, a computer emergency response team (Bimantara, 2022).

From the Australian perspective as it pertains to some academics, the focus shifts from primarily dealing with establishing norms and rule of law as is the case with the Chinese perspective, and from dealing partially on the promotion of rule of law is is the case with Japan, to the "development of managerial, technical, social, legal, policy, and regulatory initiatives by a growing ecology of actors to enhance the resilience of nations to cybersecurity breaches, cybercrime, and terrorism" (Dutton et al., 2019). The study undertaken by Dutton in 2019 to gauge the efficiency and value of Australia's, and every nation's cyber capacity building measures, confirmed that building cybersecurity capacity is of value to the larger economy and society as a whole, noting that elements of cybersecurity capacity have a strong impact on reducing exposure to security problems by those on the receiving end of capacity-building measures (Dutton et al., 2019).

Somewhat opposed to the other middle powers in the region, such as Japan and Australia, Canada's cyber capacity-building efforts in the region have been more normative as opposed to pragmatic. As EU Cyber Direct notes, Canada has quietly developed its own robust cyber diplomacy approach that is primarily focused on promoting a rules-based international order in cyberspace (EUCD, 2023). Canada's efforts in securing cyberspace push a strictly national security-centric outlook to the background in favor of promoting issues of human security. As noted at the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (United Nations, 2015), Canada endeavors to be able to provide a free, open and secure cyberspace, a domain that is deemed to be critical to global security, economic prosperity, but most notably given its concern for human security, the promotion of human rights, democracy and inclusion. Key efforts in cyber capacity-building measures from Canada include its partnership with INTERPOL and its respective initiatives to enhance cybersecurity through the use of forensic investigation tools and skills in Southeast Asia, as well as their The Canadian Cyber Threat Exchange, in which actionable information on cyber threats is shared amongst businesses who have dealings in Canada, and their role as a founding partner of the Global Forum on Cyber Expertise (Bhatt, 2017).

Moving Forward

Cooperation among middle powers in the Indo-Region is not an endeavor that is exclusive to states alone, as practitioners and institutions have the potential to play a meaningful role in establishing cooperation among like-minded partners at a non-state level. In order to effectively address the challenges the region faces, it is imperative to consider ways to engage non-state actors through new avenues. One promising area for cooperation among both practitioners and institutions on this front is through the establishment of university consortiums within the Indo-Pacific aimed at addressing regional cybersecurity issues. These collaborations can provide a unique platform to facilitate discourse between experts in academia throughout the region and beyond, allowing for a deeper level of cooperation between like-minded countries like those mentioned in this paper, as well as political entities such as Taiwan.

University consortiums, once established, can serve a myriad of purposes that are beneficial to all involved. Ones such as this could allow those involved to identify challenges facing the region in regard to cybersecurity, as well as identifying and sharing methods and best practices to mitigate said challenges. Moreover, such initiatives can help foster a cyber-aware culture among their members through focusing on critical areas such as education and literacy. Cooperation on identification, mitigation, defense, response and educational initiatives can serve an even greater purpose in reaching the public — vaccinating citizens in open societies against disinformation through awareness programs in schools, as well as through public awareness programs in the media. Initiatives such as this could even be grouped as minilateral engagement groups under the umbrella of larger frameworks, such as G7, or looking within the Indo-Pacific, the QUAD, with the goal of leveraging the strengths of practitioners to develop robust and collective responses to cyber issues.

Conclusion

Neo-middle-power diplomacy at its core is about enhancing strategic autonomy through pursuing pragmatic, less normative foreign policy — actively aiming to shape regional order through aligning collective capabilities and capacities. As our world continues to be affected by era-defining events such as the war in Ukraine and the COVID-19 pandemic, securing a level of safety and prosperity remains at the forefront of any foreign policy agenda. As threats to security continue to emerge year after year in cyberspace, middle powers must cooperate amongst themselves in order to adapt to and find their footing in this new reality.

Through actively pursuing cyber confidence-building measures, middle powers are able to further align themselves politically with potential allies, laying the building blocks for trust, transparency, and knowledge as to where each other's capabilities lie — enabling capabilities based cooperation to take place and for bolting on to, or even creating new diplomatic structures. Likewise, cyber capacity-building measures provide middle powers the means to enhance their engagement in the Indo-Pacific and establish deeper ties with regional partners, whether that be through a normative or pragmatic approach. Through fostering cyber capacity-building, middle powers are able to address the region's growing cybersecurity concerns, developmental divide, and infrastructure and communications gap to further build toward the goals of safety, resilience, and prosperity within the Indo-Pacific. By engaging in proactive neo-middle-power diplomacy and treating with the multitude of middle powers in the region, middle powers are able to become more effective, capable, and autonomous stakeholders.

References

ASEAN. (2022). Cybersecurity Cooperation Strategy. *NPF Publication*. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Betz, D. J. (2009). The RMA and 'Military Operations Other Than War': A Swift Sword that Cuts Both Ways. *B. F. W. Loo (Eds.), Military Transformation and Strategy: Revolutions in Military Affairs and Small States*. Routledge

Bhatt, A. (2017). Cyber Security and Sustainable Development-Strategic Policy Analysis of India and Canada. *National Law University Dehli*. SSRN 3009892

Bimantara, A. (2022). The Normative Enactment of International Cybersecurity Capacity Building Assistance: A Comparative Analysis on Japanese and South Korean Practices. Global: *Jurnal Politik Internasional*, *24*(1), 109–142.

Borghard, E. D., & Lonergan, S. W. (2018). Confidence building measures for the cyber domain. *Strategic Studies Quarterly*, *12*(3), 10–49. https://www.jstor.org/stable/26481908

Callanan, C., Chandola, B., Ebert, H., Heinl, C., & Sarma, A. (2022). Enhancing global cybersecurity cooperation: European and Indian perspectives. *Observer Research Foundation* (ORF). https://www.orfonline.org/wp-content/uploads/2022/10/ORF_Report_Cybersecurity-India-Europe.pdf

Dunn Cavelty, M. (2018). Europe's cyber-power. *European politics and society*, *19*(3), 304–320. https://doi.org/10.1080/23745118.2018.1430718

Chapnick, A. (1999). The middle power. *Canadian Foreign Policy Journal*, 7(2), 73–82. https://doi.org/10.1080/11926422.1999.9673212

DeNardis, L. (2014). *The Global War for Internet Governance*. New Haven, Connecticut: Yale University Press.

Dewitt, D., & Kirton, J. (1983) *Canada as a Principle Power*. Toronto: John Wiley & Sons.

Domingo, F. C. (2022). Making sense of cyber capabilities for small states: *case studies from the Asia-Pacific*. Routledge.

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity capacity: does it matter?. *Journal of Information Policy*, 9, 280–306. https://doi.org/10.5325/jinfopoli.9.2019.0280

Ernst, M., & Lee, S. (2021). Countering Cyber Asymmetry on The Korean Peninsula: South Korea's Defense Against Cyber Attacks from Authoritarian States. *Journal for Intelligence, Propaganda & Security Studies*, 15(1). https://doi.org/10.1007/978-3-031-08384-6_6

EUCD. (2023). *Canada*. EU Cyber Direct. https://eucyberdirect.eu/ atlas/country/canada

Fang, B. (2018). *Cyberspace Sovereignty*. Springer.

GFCE. (2020). *Overview Of Existing Confidence Building Measures As Applied To Cyberspace*. Global Forum on Cyber Expertise. https://cybilportal.org/wp-content/uploads/2020/05/GFCE-CBMs-final.pdf

Harknett, R. J. & Stever, J. A. (2009). The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal of Homeland Security and Emergency Management*, 6(1), 1–14. https://doi.org/10.2202/1547-7355.1649

Hoffman, W., & Levite, A. (2017). *Private sector cyber defense: Can active measures help stabilize cyberspace?*. Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Cyber_Defense_INT_final_full.pdf

Homburger, Z. (2019). The necessity and pitfall of cybersecurity capacity building for norm development in cyberspace. *Global Society*, 33(2), 224-242. https://doi.org/10.1080/13600826.2019.1569502

IBM. (2023). *IBM Security X-Force Threat Intelligence Index 2023*. https://www.ibm.com/reports/threat-intelligence?utm_id=SI-Blog-Inline-XFTII-2023

Kim, S. (2022). The Inter-network Politics of Cyber Security and Middle Power Diplomacy: A Korean Perspective. In S. Lee & S. Kim (Eds.) *Korea's Middle Power Diplomacy: Between Power and Network* (pp. 97–123). Springer.

Kim, S. (2014). *Roles of middle power in East Asia: A Korean perspective*. East Asia Institute. https://www.eai.or.kr/data/bbs/eng_report/20140203158563.pdf

Kimhy, E., &; Tribbey, B. (2022). A closer look at ransomware attack trends in APJ. *Akamai*. https://www.akamai.com/blog/security-research/ransomware-attack-trends

Madnick, S. (2024, February 22). *Why data breaches spiked in 2023*. Harvard Business Review. https://hbr.org/2024/02/why-data-breaches-spiked-in-2023

Malachinski, P. (2023). Japan's Indo-Pacific strategy in cyberspace. *Observatory*. https://www.sciencespo.fr/ceri/observatory-indo-pacific/wp-content/uploads/2023/06/CJ_MALACHINSKI-Piotr_Final-essay.pdf

Nagy, S., & Ping, J. (2023). *The End of the Normative Middle Power Ship: An Analysis*. Australian Institute of International Affairs. https://www.internationalaffairs.org.au/australianoutlook/the-end-of-the-normative-middle-power-ship/

Nagy, S. (2022). US-China strategic competition and converging middle power cooperation in the Indo-Pacific. *Strategic Analysis*, 46(3), 260-276. https://doi.org/10.1080/09700161.2022.2088126

Nagy, S. (2021). Function over form: Canada's bolting-in and capabilities-led approach to Quad Plus engagement. In J.P. Panda & E. Gunasekara-Rockwell (Eds.) *Quad Plus and Indo-Pacific* (pp. 177–191). Routledge.

Nagy, S. (2021). Quad Plus? Carving Out Canada's Middle-Power Role. *Journal of Indo-Pacific Affairs*, *3*(5), 179–95. https://media.defense.gov/2021/Mar/12/2002599869/-1/-1/0/11-NAGY.PDF/TOC.pdf

Nagy, S. R. (2022). Middle-power alignment in the free and open indo-pacific: Securing agency through neo-middle-power diplomacy. *Asia Policy, 17*(3), 161-179. https://doi.org/10.1353/asp.2022.0039

Nye, J. S. (2010). *Cyber power*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and implications. *International Conference on Cyber Warfare and Security*. Academic Conferences International Limited.

Paskal, C. (2021). *Oceania and Canada: Building Bridges in the Free and Open Indo-Pacific*. Canadian Global Affairs Institute. https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/4634/attachments/original/1615009156/Oceania_and_Canada_Building_Bridges_in_the_Free_and_Open_Indo-Pacific.pdf?1615009156

Patton, S., Sato, J., & Lemahieu, H. (2023). *2023 Key Findings Report*. Lowy Institute Asia Power Index. https://power.lowyinstitute.org/downloads/lowy-institute-2023-asia-power-index-key-findings-report.pdf

Ping, J. H. (2017). *Middle Power Statecraft: Indonesia, Malaysia and the Asia-Pacific.* Routledge.

Richey, M. (2022). Cyber Offence Dominance, Regional Dynamics, and Middle Power–led International Cooperation. In G. Boulet, M. Reiterer, & R. Pacheco Pardo (Eds.) *Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives* (pp. 67–97). Springer.

Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies*, *39*(1), 1–19. https://doi.org/10.53532/ss.039.01.00115

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication* (includes Communication Reports), *63*(3), 382–412. https://doi.org/10.1080/10570319909374648

United Nations. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf?token=hpvTcXWs8mmmvDfVcj&fe=true

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system.* Oxford University Press, USA.

Vosse, W. (2022). A conceptional broadening of the security order in the Indo-Pacific: The role of EU-Japan cooperation in ICT and cybersecurity. *Asian Affairs*, 53(3), 561–582.

YCAPS, (2023). Aukus and the Indo-Pacific. Online. https://www.ycaps.org/ycaps-jicuf-policy-d.

Ziolkowski, K. (2013). Confidence Building Measures for Cyberspace–Legal Implications. *NATO CCD COE Publication*, 1–88.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/