Routledge
Taylor & Francis Group

Australian Journal of International Affairs

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/caji20

Advancing cyber diplomacy in the Asia Pacific: Japan and Australia

Mark Bryan F. Manantan

To cite this article: Mark Bryan F. Manantan (2021): Advancing cyber diplomacy in the Asia Pacific: Japan and Australia, Australian Journal of International Affairs, DOI: 10.1080/10357718.2021.1926423

To link to this article: https://doi.org/10.1080/10357718.2021.1926423

Published online: 13 May 2021.

AUSTRALIAN JOURNAL OF INTERNATIONAL AFFAIRS
https://doi.org/10.1080/10357718.2021.1926423

Routledge
Taylor & Francis Group

Advancing cyber diplomacy in the Asia Pacific: Japan and Australia

Mark Bryan F. Manantan

Pacific Forum, Honolulu, HI, USA

ABSTRACT

The stability in the cyber domain is rapidly deteriorating on several fronts marked by increasing sophistication of cyberattacks, declining consensus on global internet governance and intensifying great power competition. These challenges were critical turning points among nation-states to recalibrate prevailing cyber diplomatic engagements. This article investigates the increasing prominence of deterrence in the practice of cyber diplomacy in the Asia Pacific. Using Japan and Australia as case studies, it argues that both states continue to adhere to the conceptual tenets of cyber diplomacy, however, in practice, there is a growing integration of deterrence—cyber capabilities and public attribution/naming and shaming—in the equation at varying degrees and intensities. The article endeavours to make two important contributions: First, revitalize the existing cyber diplomacy framework by challenging the extant literature's view of deterrence's limited application—underpinned by cold war analogies—and the implausibility of conducting attribution of cyberattacks. Secondly, evaluate Japan and Australia's cyber diplomacy based on empirical evidence. Key findings suggest that deterrence reinforces/complements the fundamental elements present in the cyber diplomacy playbook. While slight variation exists, there is a strong acquiescence between Japan and Australia to expand existing cyber cooperation to tackle critical and emerging technologies, supply chain, and data governance.

KEYWORDS

Cyber diplomacy; Japan; Australia; cyber deterrence; cybersecurity

Introduction

The state of international cybersecurity cooperation is heading towards heightened uncertainty. The source of political and diplomatic volatility stems from the intensifying techno-nationalism triggered by the US–China strategic competition (Tao and Woo, 2018), and the poor appetite towards a united consensus on global internet governance (Grigsby 2017). Further exacerbating such anxiety are the increasing sophistication and magnitude of cyberattacks, and the disruptive effects of technological innovations. The Asia Pacific—home to the world's rising digital economies—is at the frontline of such alarming cyber insecurity. As the region reaps the economic benefits of the Fourth Industrial Revolution, its increasing reliance on Information and Communication

CONTACT Mark Bryan F. Manantan mark@pacforum.org; bfmgrey@gmail.com
This article has been republished with minor changes. These changes do not impact the academic content of the article.

Technologies (ICT) have also left it very exposed from new breeds of risks and vulnerabilities (Segal *et al.* 2020). With limited or even absent capacity to address cyber threats, nation-states in the region were encouraged once again to step up in their cyber capacity-building at the country and regional-level (UNESCAP 2020).

As two of the most technologically advanced economies in the Asia Pacific, Japan and Australia have been actively responding to such call for improved cyber diplomacy. Both countries echoed a shared commitment in advancing cooperation to maintain stability and sustain multilateral consensus in cyberspace. In their 2019 Cyber Policy Dialogue, Japan and Australia

> reaffirmed their commitment to continue to enhance cooperation and information sharing on responses to malicious cyber activities, including deterring and responding to significant cyber incidents … strengthen[ing] the strategic framework of international cyber stability … [and] to work collaboratively on cyber capacity building across the region. (Cyber Affairs 2019)

Individually, both countries are also pursuing similar approaches—Australia has recently released its latest *2020 Cyber Strategy* with an increasing emphasis on 'deterrence', while Japan's steady rise as a cyber power presents a more defensive outlook in cyberspace (Bartlett 2020). These parallel developments underscore the increasing nexus of cybersecurity and diplomacy in the Japanese and Australian foreign policy particularly in their engagements towards Southeast Asian and Pacific Island nation-states.

The modest aims of the article are: first, investigate the evolving concept and practice of cyber diplomacy in the Asia Pacific in the context of Japan and Australia. Specifically, the article will explore the rationale behind the two countries' dynamism in such burgeoning areas of diplomacy over the last decade. Secondly, it will examine the growing salience of deterrence in the cyber diplomacy literature. As briefly mentioned in Japan and Australia's joint-statement, the notion of deterrence—potentially through cyber capabilities and the use of public attribution or naming and shaming—is becoming a prominent dimension in their diplomatic maneuvering in the cyber realm. This raises an important gap in the broader cyber diplomacy framework as the prevailing literature consider deterrence as less convincing and ineffective due to: (i) its limited application in the cyber domain, (ii) the attribution problem, and (iii) its potential to trigger a cyber arms race (Barrinha and Renard 2017; Meer van der 2016; Riordan 2019). However, a deep dive into the growing practice of cyber diplomacy particularly in the Asia Pacific proves otherwise.

To this end, I put forward the argument that Japan and Australia's cyber diplomacy adheres to the broad conceptual tenets of the prevailing cyber diplomacy framework but in *practice*, both countries are integrating deterrence in the equation at varying degrees. Japan and Australia were chosen as key analytical subjects as they sit comfortably at the interstices of the ongoing deterioration of cyberspace. Considered as second-tier or middle power states in the international world order, they bear the brunt of the intensifying US–China great power competition due to their interdependence with the two powers as well as their deeply-entrenched interests towards the enduring stability of the current *international rules-based order*. Given their limited material capabilities compared to the US and China, and normative proclivities to support multilateral diplomacy in the Asia Pacific, they present a unique case in cyber diplomacy. They adopt a dual-track approach of cooperation and competition, striking a balance between

defending themselves from urgency poised by cyber insecurity, while still mindful about the preservation of multilateral avenues for dialogue and collaboration. In this regard, they are the ideal case studies to explore the article's main argument due to their nimbleness to recalibrate cyber diplomatic engagements contingent on the challenges of the deteriorating cybersecurity cooperation. Although there is a minor distinction, their dual-strategy underlies a common approach: fortifying deterrence capabilities on one hand, while using capacity building and confidence-building measures to avoid escalation or perception of cyber arms race on the other.

In probing the case studies, the article also explores three explanatory factors at play that influenced the growing salience of deterrence in Japan and Australia's cyber diplomacy toolbox: The confluence of the political-security environment in the Asia Pacific region, marked by (1) China's rise juxtaposed by the (2) potential disengagement of the US; (3) the evolving and transnational nature of cyber threats and the need to buttress regional and multilateral cyber dialogue. In examining the practice of cyber diplomacy by Japan and Australia, the study endeavours to make two important contributions. First, elucidate the increasing emphasis on deterrence measures as signalling tools that could offer insights in revitalizing the existing cyber diplomacy framework. Secondly, evaluate the distinct characteristics and/or overlaps on the empirical practice of Japan and Australia's cyber diplomacy. Data for this article was derived from primary interviews with cybersecurity policy experts and foreign affairs officers as well as secondary sources such as academic and journal publications, government reports, policy papers, and media articles.

The key findings of the study suggest that contrary to the prevailing literature that deterrence lends itself ineffective due to issues relating to attribution and prevailing cold war analogies, its undervalued merit lies in its capacity in shaping the normative and operational contours of the cyber domain. As the global consensus on internet governance remains elusive at least in the short to medium term, exacerbated by the instability emanating from the great power contest and the evolving cyber threat landscape, nation-states such as Japan and Australia will continue to exercise a high degree of agility in refining their cybersecurity statecraft to include elements of deterrence to deal with unpredictable security and political environment. While slight variation exists in their practice, there is a strong convergence between the two countries to lead efforts that guarantee a more stable cybersecurity ecosystem in the Asia Pacific.

To illuminate the overall argument, the article shall take four steps: first, in the proceeding section, the article will tackle the conceptual framework of cyber diplomacy and locates the increasing salience of deterrence in the cyber diplomacy literature. Afterward, the second section expounds on the explanatory factors which contributed to the rapid integration of deterrence in the cyber diplomatic engagements of Japan and Australia. To ground the reconceptualization of the cyber diplomacy framework on empirical facts, the third section offers an in-depth examination of the Japanese and Australian case studies. The final section concludes.

Defining cyber diplomacy

The scale and speed of technological advancements in cyberspace are unprecedented. As the fourth industrial revolution dawns, bringing with it the reality of Big data, Artificial

Intelligence, and quantum technology, the world is entering a new level of more sophisticated hypoconnectivity, blurring the nature of interaction and exchange between offline and online communities. The role of the new cyber frontier is significant for the way that nation-states conceptualize their interests in a contemporary world. It is somewhat of an Achilles heel for governments who seek to mitigate its threats while maximizing the opportunities it offers. As the possibilities for innovation in cyberspace grow so too does the potential for competition and to some extent, conflict.

States are gradually focusing their attention on policy mechanisms that might promote and safeguard their interests within the cyber domain. Many policymakers grappling with the uncertainty of this uncharted territory are also cognizant of the urgency underpinning the need for shared and accepted rules, protocols, and behaviours that will facilitate smooth interactions between global actors within it (Meyer 2015; Nye 2010). Diplomatic practice is central in laying the groundwork for cooperation among state and non-state actors within an interest in cyberspace (Hocking *et al.* 2012; Meyer 2012).

However, diplomatic approaches towards cyberspace are fraught with complicated challenges. Compared to traditional domains of land, air, and sea, where diplomacy has neatly laid the bedrock of state's normative interaction, cyberspace is both complex and continuously evolving (Betz and Stevens 2011, 43–44). Despite the commonly held notion that cyberspace belongs to the 'global commons', cooperation in this area has been fragmented and ad-hoc (Henriksen 2018; Mueller 2017). The intangible and ever-changing nature of cyberspace, which has attracted a mix of actors with varying normative and ideological motives, suggests the need for coherent multi-stakeholder diplomatic approaches that are innovative, agile, and adaptive. Thus, the concept of 'cyber diplomacy' has become an emerging frontier to develop cooperation and interoperability in such a contested space.

Cyber diplomacy is broadly defined as the use of diplomatic tools and initiatives to achieve a state's national interest in cyberspace that are commonly crystallized in the national cybersecurity strategies (Barrinha and Renard 2017; Riordan 2019). Cyber diplomacy encompasses a wide range of diplomatic agenda such as (1) establishing communication and dialogue between state and non-state actors; (2) prevention of a cyber arms race; (3) development of global norms; and the (4) promotion of national interests in cyberspace through cybersecurity policies and engagement strategies (Barrinha and Renard 2020, 12–16). It also focuses on the evolving roles of diplomats and the reorganization of various departments and ministries of Foreign Affairs to cater to the rising prominence of cybersecurity in the pursuit of foreign policy (Barrinha and Renard 2020; Riordan 2019) or the role of new technologies in the processes and structures of diplomacy (Kleiner 2008; Potter 2002).

Cyber diplomacy is informed by multiple dimensions of soft power and is considered an effective solution in mitigating the outbreak of massive political or economic uncertainties, risks, and potential conflicts emanating from cyberspace (Meer van der 2015). Fundamental elements in the cyber diplomacy toolbox are *cyber capacity-building, confidence-building measures, and the development of cyber norms*.

Capacity building in cybersecurity is motivated by the ultimate goal of deterring threats (Calderaro and Craig 2020, 8). States are developing the cyber capacity to reduce cyber-related as well as conventional threats posed by rival actors (Calderaro and Craig 2020, 8). It involves the diffusion of technical, governance, and diplomatic

expertise required to ensure resilience against online threats, encompassing the enactment of national cybersecurity strategies, the establishment of computer incident response teams, and the strengthening of law enforcement bodies (Calderaro and Craig 2020, 6). However, the dimensions of the capacity building have evolved beyond standard technical considerations or regulatory frameworks to include raising education and awareness (Dutton et.al, 2019). As the nature of cyber threats knows no borders, capacity building emerged to aid developing economies facing various security challenges due to uneven or lack thereof of technical skills and resources. Addressing such debilitating condition requires human resource development, institutional and organization reform, private-public cooperation, and access to internet connectivity itself (Muller 2015; Pawalk and Barmpaliou 2017).

Confidence-building measures (CBMS) in the cyber domain enable greater information-sharing to mitigate uncertainty, enhance predictability and transparency on motivations and intent, and facilitate crisis management or remediation strategies among states. As cyber activities are cloaked in secrecy, CBMs provide mechanisms to prevent and regulate certain behaviour by reducing ambiguity and suspicion (Meyer 2011). Information-sharing in CBMs revolve around threat actors' profile; tactics, techniques, and procedures, (TTPs), systems and vulnerability disclosures; as well as the publication of cyber doctrines and national cybersecurity policies (Borghard and Lonergan 2018, 21–22). CBMs are also paving the way in the promotion of cyber norms by establishing shared expectations on nation-states' acceptable conduct as well as mitigating a cyber arms race in the development of capabilities (Borghard and Lonergan 2018, 21–22).

Cyber norms are defined as the 'standards of appropriate behaviour concerning the use of ICT' in the context of maintaining international stability and security, (Maurer 2020, 5). They are 'voluntary, nonbinding norms as an alternative to law' (Finnemore and Hollis 2017, 442). Conversely, International law can serve as a basis for cyber norms, and cyber norms can be codified into international law for cyber conflict or cyber warfare as exemplified in the Tallinn Manual (Finnemore and Hollis 2017, 442).

Amid increasing cyber-attacks to critical infrastructures, data breaches, cybercrime, cyber espionage, online theft and pilferage of trade secrets, and offensive cyber operations carried out by state or non-state actors, cyber diplomacy can mitigate cyber aggression or the escalation of conflicts (Meer van der 2016). The hyperconnected and transboundary nature of cyberspace makes it critical for states to develop and engage in cyber diplomacy rather than exclusively rely on cyber defense (Gady and Austin 2010, 1). Through capacity-building initiatives and CBMs, state and non-state actors may be able to establish an atmosphere of predictability and transparency (Meer van der 2016). And with the constant interaction and on-going collaboration in such areas, the potential creation and adoption of cyber norms that regulate responsible state behaviour become feasible over the long term (Meer van der 2016).

The past decade has seen a rise in the call by states for more cooperative cyber diplomacy strategies.[1] Most notable among these cyber diplomacy efforts was the US–China Cyber Agreement in 2015 entered by President Barack Obama and President Xi Jinping. The agreement led to the reduction of Chinese cyber-espionage activities along with a recalibration of cyber policies on the part of Beijing which led to a friendlier US–China cyber relation (Chua 2017). Additionally, non-state actors including multinational and private companies are also actively engaged in the cyber diplomacy discourse (Hurel

and Lobato 2018). Microsoft boasts its own Global Security Strategy and Diplomacy Team, while Huawei has collaborated with Microsoft and East–West Institute to develop standards to influence ICT procurements (Segal 2017, 14). Despite being sub-state actors, such ICT companies are exuding diplomatic agencies to promote cyber norms.

But despite the positive momentum in cyber diplomacy among individual state and non-state actors, underlying tensions at the multilateral level have stalled cooperation especially on critical issues of further developing cyber norms and the applicability of international law in cyberspace. In 2017, the UN Group of Government Experts (GGE)—the central body tasked to improve the stability of cyberspace and minimize the risk of outright conflict—hit a roadblock. Following a positive track record of its reports being adopted in 2010, 2013, and 2015, the UN GGE was unsuccessful in 2017 to release a document clarifying the application of international law in cyberspace (Henriksen 2018).

The collapse of the UN GGE talks illustrates the brewing contestation between western democracies and authoritarian camps stemming from their differing views on the application of the right to self-defense, international humanitarian law, and the use of countermeasures in cyberspace (Grigsby 2017, 113). Two major factors led the UN GGE to hit a dead-end. First, while the US advocates on *constraining* cyber-based conflict, Russia and China are more concerned about *preventing* the occurrence of conflict in the first place. Russia and China believe that the US could potentially use international law to justify the use of cyberweapons in the event of an armed conflict. Secondly, the US, Russia, and China fundamentally diverge in identifying the nature of cyber conflict itself (Grigsby 2017, 114).

The fallout revealed the deep-seated fundamental divide between the US and its allies versus Russia and China grounded on their diverging ideological proclivities on the broader aspect of internet governance. On one hand, Western democracies led by the US advocate for a multi-stakeholder approach that champions inclusivity of participation in the promotion and adoption of international norms and rules, particularly the free flow of information. On the other, Russia and China are more concerned about maintaining information control for the sake of national security which falls under their notion of cyber sovereignty (Kim 2014, 331). This growing divide thus makes a strong case for the potential balkanization of the internet marked by the rise of digital borders between those who espoused cyber sovereignty versus the free and open flow of information (Hill 2012). The underlying logic behind the so-called 'Splinternet' phenomenon also reveals the simmering battle for global technological supremacy between the US and China (Kennedy and Lim 2018). It is no secret that China continues to advance its efforts in technology standard-setting to challenge and eventually replace the rules and principles governing the internet which were predominantly established and influenced by the US. If successful, this could lead to the proliferation of decentralized internet infrastructure, giving birth to a 'Western' and 'Eastern' version of the internet ecosystem (Hoffmann, Lazanski, and Taylor 2020, 252–253).

Therefore, the path towards developing cyber norms that will promote and preserve more stable and secure cyberspace remains desolate. As the current relationships among the US, China, and Russia continue to deteriorate, the momentum for the great powers to come to the table is nowhere in sight. This makes the prospect for

cooperation among the perceived 'gatekeepers' of the cyber domain highly implausible (Finnemore and Hollis 2020, 454), and thus, challenging the argument that cyber norms presents the most realistic pathway in addressing cyber threats (Mazanec 2016). Recognizing the uncertainty and challenges on the progress of international cyber norm-making, compounded by the evolving threats and changing vulnerabilities in cyberspace, states are devising a panoply of diplomatic tools and initiatives in cyberspace with an increasing emphasis on cyber deterrence.

Understanding deterrence in cyberspace

The idea of cyber deterrence rests on the capacity of a nation-state to disincentivize hostile actors in launching cyberattacks. It shapes the underlying motives and/or the cost–benefit calculation among adversaries on the perceived costs and risks in conducting cyber operations (Libicki 2009, 28). At the bare minimum, cyber deterrence can diminish 'the risk of cyberattacks at an acceptable level at acceptable cost' or put simply, mitigate the cost of defending systems (Libicki 2009, 32–37). Although the concept is applied in cyberspace, cyber deterrence could be used in concert with all the other available resources—diplomatic, information, military to economic—at varying intensities and consistent with international law (Nye 2017, 46). Cyber deterrence fits neatly within the state's overall deterrence strategy and can be used in coordination with other suite of kinetic tools (Nye 2017, 55).

There are two major types of deterrence in cyberspace: Deterrence by Punishment and Denial. *Deterrence by punishment* means there will be significant retaliatory response/s against any adversary in the event of an attack (Knopf 2013). It raises the costs against the perpetrator of cyberattacks through possible retribution via cyberweapons, along with conducting offensive cyber operations to exploit vulnerabilities towards an adversary's networks to mount an imminent attack. The deterrent effect as far as cyber capabilities is concerned is dependent on three factors: the strategic doctrine underpinning its use, the awareness of others, especially adversaries about its existence, and the potential use of such capabilities (Limnell 2016, 55). Overall, the demonstration of a state's resolve to use its cyber capabilities is necessary for it to acquire deterrence currency (Limnell 2016, 55). Deterrence by punishment in cyberspace could also involve intra-domain retaliation based on a graduated level of responses from diplomatic, economic, physical to nuclear force (Libicki 2009, 26, 29) or it could also be combined with economic sanctions or a joint-cyber and kinetic attacks (Lupovici 2011, 54). In 2015, the US has imposed the first unilateral sanction against North Korea following its cyber-attacks on Sony Pictures (Francis 2015). Conversely, in 2017 the EU launched its *Cyber Diplomacy Toolbox* that emphasized the imposition of sanctions to influence the behaviour of cyber aggressors (Moret and Pawlak 2017, 1). Sanctions could be employed as signalling mechanisms to deter and demonstrate a strong resolve towards initiating a proportionate response against nefarious actors engaged in such malicious activities (Moret and Pawlak 2017, 2).

Deterrence by denial is more defense-oriented which aims to dissuade any attacker that its efforts to infiltrate will fail (Knopf 2013). Additionally, it does not only convince the attacker to give up its cause but also it involves hardening the necessary cyber defenses to mitigate any possible breach on the part of the target (Lupovici 2011, 54). In short, denial consists of prevention and futility. The use of defensive measures can reduce the

probability or could even disrupt the attack in the process. And even if the attack is carried out, the desired effects against the target will not eventuate (Goodman 2010, 106). Related concepts to deterrence by denial include resilience or the ability to withstand any disruptive effects from cyberattacks (Geist 2015, 56) as well as the practice of good cyber hygiene to obstruct and even enhance extended deterrence particularly in the context of non-state actors such as the private sector (Nye 2017, 57).

Although the concept of deterrence is predominantly classified under the two categories of punishment and denial, Nye (2017, 58) broadened the concept to include two political mechanisms: entanglement and norms. *Entanglement* refers to how the interdependencies which exist between the attacker and its target could influence its cost–benefit analysis in launching an attack (Nye 2017, 58). Deterrence is achieved when the attacker reconsiders its actions given the significant cost it could impose on its relationship with the target or to the prevailing status quo (Nye 2017, 59). As Nye pointed out, the deterrent effect of entanglement would work well for the US and China given their deeply intertwined economic interdependence, but not as much with countries with asymmetrical dependencies such as the US and North Korea (Nye 2017, 58). Meanwhile, *Norms* can deter the actions of the attacker given the possible reputational damage against its soft power status. Like entanglement, there are social costs imposed against the attacker even with no evidence of defense or retaliation from the target (Nye 2017, 60). Moreover, a norms-based approach in cyber deterrence shapes the rules of the road especially for the defensive and offensive use of *cyber* weapons to prevent cyber arms race (Stevens 2012). The notion of *naming and shaming* also known *as public attribution* falls within this category where actors who are transgressing implicit norms lose face (Nye 2017, 66). It serves as a signalling tool against an adversary that it has been caught, which in the longer-term consequently shapes the future political and normative operational terrain (Egloff 2020). Public attribution could either be conducted independently by a state or set in a broader political coalition. In this regard, actors who invoke the 'name and shame' card achieve a degree of deterrence against adversaries while in the process, reinforce and even construct new norms including international law (Egloff 2020; Finnemore and Hollis 2020).

Applying the principle of deterrence in the cyber realm has also been fraught with immense challenges, primarily due to the influence of Cold War analogies over the effectiveness of the concept and compounded by the issue of attribution (Clarke 2016; Iasiello 2014). The current conceptualization of deterrence shaped during the nuclear arms race is not in sync with the structural and operational characteristics of the cyber domain. Cyberspace is highly interconnected; the barriers to entry are low allowing both nation-state and non-state actors to exert influence; and damage can be inflicted below the threshold of conflict which does not trigger a kinetic response (Fischerkeller and Harknett 2017).

Relatedly, there is the issue of attribution. Actors in the cyber domain also operate in such a highly ambiguous fashion, making any attempts in establishing clear communication difficult which might result in misinterpretation or even miscalculation (Iasiello 2014, 56–57). Attribution requires a more nuanced process beyond conducting technical analysis as it entails a high degree of confidence in determining the culprit of the attack. As the process involves the timely collection and analysis of forensic evidence, the difficulty lies in establishing accuracy to avoid any false flags or result in misattribution

(Iasiello 2014, 58). Unless a certain degree of attribution capabilities can be employed to nefarious actors, deterrence will not work (Lindsay 2015). In this regard, the inherent characteristics of the cyber domain marked by anonymity and interconnected yet scattered networks with a global reach renders cyber deterrence strategy useless (Lan *et al.* 2010). With these features, the core elements of deterrence—attribution, defense, and retaliation, and signalling—developed during the Cold War era will not function well to address the very nature of the cyber conflict (Taddeo 2018).

In defense against the criticisms levied on the limited effectiveness and application of the deterrence framework in the cyber domain, various scholars have recast it into a new light away from its Cold war trappings. As Tor (2015) claims, applying the concept of 'total or absolute deterrence' in cyberspace borrowed from the nuclear deterrence model is ill-fitted in such a domain. Absolute prevention of cyberattacks is near-impossible, and thus, the notion of a 'cumulative deterrence'—the use of 'short bursts of force' to minimize damage and shape the cost–benefit calculation of rivals—presents a more pragmatic reconceptualization of deterrence in the emerging domain (Tor 2015, 11–12). Similarly, Kello (2017) also suggested 'punctuated deterrence' or a series of actions that produce a cumulative effect rather than a tit-for-tat response. Compared to Nuclear deterrence, which is implemented in a singular and symmetric fashion, cyber deterrence is repeatable, asymmetric, and could involve non-kinetic interventions (Libicki 2009). Jensen (2012) claims that cyber deterrence is far more flexible than the original deterrence concept, imbued with additional tools of International law and networks and systems resiliency. This makes it more interdependent with other elements of diplomacy and international law rather than the nuclear era's all-or-nothing approach. And although deterrence does not fit neatly on the operational characteristics of the cyber domain, its effect in establishing good practices, and shaping the discourse on international norms and responsible state behaviour cannot be ignored (Miadzvetskaya 2021).

Those disputing the inherent analytical power of deterrence must also widen their aperture. Contrary to the one-dimensional application of nuclear deterrence, the cyber environment is highly interconnected, cutting across various domains, from the physical to the digital sphere (Goodman 2010). Rather than narrowly fixating on the domain-specific characteristics where the notion of deterrence has been applied in the past, it is crucial to situate cyber deterrence on a continuum and examine its practice to determine its success in deterring adversaries (Goodman 2010). Wilner (2020) claims that practice is outpacing the academic study of deterrence in cyberspace, as 'tactics, strategy, doctrine, and policy are developed and put to use even before corresponding theories are properly understood'. In effect, the insights obtained from the practical application of cyber deterrence demonstrate its viability and effectiveness, leading to the refinement of the cyber deterrence theory (Wilner 2020). By investigating its practice, scholars and policy analysts could demystify the limited depth of prevailing cold war orthodoxy towards deterrence to illumine its inherent value in the cyber realm.

Expectations underpinning attribution must also be met with pragmatism as 'successful technical attribution with a high degree of confidence may never be universally possible' (Solomon 2011, 8). The imperfect process underlining attribution does not reduce the desired deterrent effect (Nye 2017, 52). The central issue of anonymity in the attribution problem also does not perfectly apply to nation-state actors due to strategic,

contextual, and operational indicators that would limit the numbers of probable perpetrators based on the rationale of their actions or current geopolitical climate (Manantan 2020a; Tor 2015). As Rid and Buchanan (2014) argued based on observed practice, governments with a vast number of technical resources and skilled manpower can conduct covert operations, uncover enemies, and respond accordingly. This makes attribution with a relatively high degree of confidence feasible. Therefore, attribution is painstakingly challenging and costly but not impossible.

Evaluating the current debates surrounding cyber deterrence, this article asserts that there is a growing relationship between deterrence in cyberspace along with economic sanctions, conventional military intervention, and even nuclear force. As repeatedly stated, the notion of deterrence in cyberspace is not confined to the man-made domain itself but can be combined or complemented by the other assets available at the disposal of the state. In the interest of this article, I contend that deterrence can be used in conjecture or even integrated into the cyber diplomacy toolbox as reflected by its ongoing practice. The article, therefore, challenges the 'purist' nature of the extant literature on cyber diplomacy which discounted the role of deterrence. Contrary to Barrinha and Renard's argument (2017, 357) which dismissed the inherent value of 'deterrence … due to problems with attribution' or Meer's critique of its credibility and lasting impact (2016, 101), I take the view that overlooking the burgeoning integration of deterrence in the cyber diplomacy framework by relying too heavily on cold war analogies and the flawed notion of perfect attribution is extremely counterproductive. These assertions do not enrich the theoretical foundations of cyber diplomacy. As I argued, it is critical to assess the observed practice which could offer insights to further bolster its conceptual underpinnings.

Having reviewed the four types of deterrence in cyberspace, the study will focus primarily on the deterrent effects derived from the two mechanisms in the analysis of this article:

(1) Cyber capabilities—(i) development and acknowledgement of its possession; (ii) the corresponding strategic doctrine and legal framework underpinning its use and (iii) the potential use of the cyber capabilities for offensive and/or defensive purposes.
(2) Public attribution—the reputational costs inflicted to the adversary or perpetrator and its shaping effects in reinforcing norms, international law, and more broadly responsible state behaviour.

This article advances the argument that the integration of such deterrence mechanisms complements or reinforces the established elements in the cyber diplomacy toolbox—capacity building, confidence-building measures, and cyber norms. These tools might be deployed by states separately, but each could also be mutually reinforcing. For instance, when states acknowledge their possession or use of cyber capabilities through their strategic doctrines, such pronouncements are complemented or reinforced by CBMs through communication channels and cyber dialogues, to maintain transparency and predictability. As already mentioned, the reputational consequence of public attribution puts the onus towards the attacker to act in accordance with international law, and therefore, reinforces cyber norms of responsible behaviour in cyberspace. Likewise, capacity-building exercises encompassing the provision of cybersecurity skills and

technical resources, improving information-sharing, and strengthening cyber defenses produce a cumulative deterrent effect in mitigating cyber threats. The integration of deterrence mechanisms can augment the 'here and now' challenges in cybersecurity, especially the urgency to respond or defend against cyber-attacks in real-time, while simultaneously reinforcing the 'rules of the road' despite the absence of multilateral consensus on internet governance.

Structural factors driving Japan and Australia's Cyber diplomacy

The practice of cyber diplomacy that emphasizes deterrence is already evident in the Asia Pacific especially among Japan and Australia who have publicly reaffirmed their commitment to supplement their existing cyber diplomacy efforts with deterrence strategies. Japan's rise as 'cyber power' was indeed telling given its pacifist constitution, reflecting the urgency for Tokyo to adopt a more proactive posture in cyberspace under the conditions of international law (Kallender and Hughes 2017). While Australia's *2020 Cybersecurity Strategy* puts deterrence front and centre with its emphasis on the possible use of offensive and defensive capabilities to deter malicious actors. This section examines the structural conditions in the region that has triggered Japan and Australia's active cyber diplomacy. Three main challenges prompted the recalibration of the two countries' cyber diplomacy efforts: the emergence of great power competition, evolving transnational cyber threats, and the impasse in global governance. The combined impact of these factors underscored the growing instability and disruptive effects of the changing cyber threat landscape, demanding a renewed call for cyber cooperation at the regional and global stage.

But before turning to the three explanatory factors, it is critical to first revisit the rationale underpinning Japan and Australia's cyber diplomacy. To understand the cyber diplomatic roles executed by second-tier or middle power states like Japan and Australia in the international system, this article adopts Sangbae Kim's (2014, 325) network perspective which advances a 'positional approach'. According to Kim, rather than looking into the internal 'attributes or capabilities', a state's network position in the international system is a far more precise barometer to explaining the roles and policies pursued by states. By zeroing on the structural conditions instead of the fixed internal attributes, the dynamic interactions among states are captured which could better explain the prevailing 'social relationship' that undergirds the entire system as a whole (Kim 2014, 327). Through occupying a strategic node at the interstices of the network structure, middle powers pursue three distinct roles: brokering, coalition-building, and programming. *Brokering* pertains to the bridging of existing structural gaps or holes; *Coalition-building* is the ability to collect and attract like-minded states or allies in pursuit of shared interests and lastly; *Programming* refers to complementing or shaping the whole system which is largely influenced by great powers (Kim 2014, 328).

With the article's identification of the three structural conditions in the cybersecurity domain, the positional approach, thus, serves as a more prescient lens to explicate the relational context upon which state actors operate. Using the network perspective, the following discussions will assess the underlying logic behind the increasing salience of deterrence in Japan and Australia's respective cyber diplomacy to contend with the structural challenges.

China's cyber threat

China's global rise has been predicated on its longstanding industrial cyber espionage campaigns against the United States to siphon intellectual property that feeds its hegemonic status and expands its regional and multilateral influence (Iasiello 2016). Like the US, Japan is no stranger to Chinese-linked cyber-attacks affecting all levels of government institutions, private companies, academia, and civil society. Japan's crown jewels—defense technologies and industries, military contractors, and finance and high-technology sectors—have been the primary target of various state-sponsored hackers linked to China (Kallender and Hughes 2017). But aside from its alleged interest to steal proprietary information to advance its technological innovation footprint, China seeks to obtain a strategic advantage over Japan through cyber espionage on major geopolitical fault lines such as the dispute on the East China Sea and its on-going relations in the Korean Peninsula (Gady 2017; Kallender and Hughes 2017; Soesanto 2020). Although North Korea and Russia were also linked to several cyberattacks, China was identified as the most prominent actor. In 2013, Japan's Ministry of Defense published the *Defense of Japan White Paper*, claiming that China's People's Liberation Army's (PLA) cyber unit was behind numerous Advanced Persistent Threats (APT) campaigns following Japan's acquisition of the disputed Senkaku/Diaoyu Islands (Kallender and Hughes 2017, 5). The rising concerns over Chinese-linked APT and the PLA's cyberwarfare capabilities prompted Japan to elevate cybersecurity as a significant national security concern alongside weapons of mass destruction and international terrorism at a regional and global scale (Kallender and Hughes 2017, 6).

Similarly, China was also behind Australia's high-profile commercial cyber espionage activities, noting Beijing's use of sophisticated cyber capabilities to advance its strategic hand over Australia's mining industry (Segal *et al*. 2018; Thompson 2012). Chinese-sponsored cyber intrusion has become unprecedented over the past decade, revealing significant concerns about China's intention not only to obtain trade secrets or geopolitical intelligence but also to undermine and influence its democratic processes (Hamilton 2021). Recognizing China's covert efforts to influence the Australian public, media, and its government led to the introduction of the Foreign Interference laws in 2017 (Brew 2019). According to Former Prime Minister Malcolm Turnbull such a new measure, in addition to its growing cyber capabilities, will protect Australian democracy from foreign interference as cybersecurity has become 'the new frontier of warfare' (Belot 2017).

US disengagement?

China's malfeasance in the cyber realm was juxtaposed by the second structural challenge: the apparent withdrawal of the US from its leadership role in various regional and global initiatives under a deeply polarizing and isolationist Trump administration. Trump's withdrawal from the Transpacific Partnership, Iran Nuclear Deal, and the Paris Climate Agreement raised doubts over the continuing commitment of the US to maintain a viable economic and strategic presence in the Indo-Pacific (Manantan, 2020b). Trump's rhetoric of criticizing US allies in the Indo-pacific on unfair trade practices and free-riding caused some initial stress over Japan and Australia (Smith and McClean 2017; Tow 2017). Trump however did very little to reorient the strategic alignment of Japan and Australia away from the US. But the 'Trump effect' resulted in both Japan and Australia pursuing more

proactive defense and security policies to reinforce or maintain active US engagement in the region (Heazle and Tatsumi 2018; Liff 2019).

Although the US remains a key plank of the two countries' security policies, undoubtedly there is an increasing convergence between Japan and Australia that solidified the notion of 'intra-spoke' cooperation (Manantan 2020b). The permutation of Trump's unpredictability and the challenges presented by growing cyber(in)security forced Japan and Australia to gradually embrace more self-reliant posturing on cyber capabilities to ward off potential adversaries, rather than relying solely on the US umbrella of extended deterrence in cyberspace under their respective treaties.

The brokering and programming efforts of Japan and Australia also became evident as they fill in the gap left by the US and counter China's increasing clout in Southeast Asia (Manantan 2020b). According to cybersecurity experts in Southeast Asia, Japan and Australia embarked on cyber capacity-building and CBM engagements in the region to sustain the US' technical and policy engagements established during the Obama era.

Transnational nature of cyber threats and impasse on internet governance

The heightening ideological and technological competition between the US and China has forestalled the progress of cyber norms and international law, further undermining stability in cyberspace. With its international dimension, cybersecurity threats cannot be solved in isolation, and the repercussions of cyberattacks are boundless (Deibert 2012). As cyberspace cuts across borders whether, through data passing from one server to another, traversing via submarine cables, or the assembly line in the critical supply chain, the entry points for malicious actors are diverse (Noor 2015). Add to this the potential spillover effects of cyberattacks which could transcend physical and virtual borders as exemplified by the WannaCry and NotPetya attack.

In this regard, a regional organization such as the Association of Southeast Asian Nation (ASEAN) has been at the apex of Japan and Australia's cyber diplomacy to augment the region's overall cyber strategic mindset and technical capabilities in deterring cyber threats (Noor 2015). ASEAN serves as an important avenue to resume and reinforce discussions on cyber norms and international law as the multilateral consensus remains in limbo. An underlying commonality exists in Japan and Australia's cyber diplomacy agenda as exemplified by their respective efforts of rallying like-minded states in the region who share the same mutual goals of reaping the benefits of a secure cybersphere.

In the proceeding section, Japan and Australia concretely demonstrate their goal of sustaining regional dialogue despite the impasse at the global level. As a testament to their programming abilities, they sought to reignite cooperation through their cyber dialogues. Japan and Australia continue to see the value of ASEAN as the neutral ground for dialogue which could potentially set in motion the momentum to revive conversations on cyber norms and International law.

Cyber diplomacy in practice: Japan and Australia

Following the discussion on the explanatory factors that underpin Japan and Australia's integration of deterrence in their cyber diplomacy playbook, this section will provide the empirical evidence which grounds the overall thesis of this article.

In what follows, I argue that from a broad perspective it appears that Japan and Australia have accelerated the integration of deterrence in their respective cyber diplomacy playbook. And in the process, the fundamental elements—capacity building, CBMs, cyber norms—are also recalibrated to reinforce or complement the integration process. But upon zooming in, the development of cyber capabilities and the use of the attribution card varies between Japan and Australia due to underlying political, strategic and diplomatic circumstances faced by both countries. While Australia have more liberty to developing offensive and defensive cyber capabilities and can conduct naming and shaming on its own terms, Japan is far more circumspect, discreet and to certain degree, restrained in both areas.

Nevertheless, in both cases studies, there is still a strong mutual link between deterrence capabilities and conventional cyber diplomatic engagements aimed at achieving maximum net-positive deterrent effects while still cognizant of avoiding any miscalculation or escalation of conflict in support of the normative dimensions in cyberspace.

Japan

As a broad overview, Japan's Cybersecurity diplomacy has identified three primary pillars: (1) promotion of the rule of law in cyberspace, (2) development of CBMs and, (3) cooperation on capacity building. Over the years, Japan has engaged proactively in promoting the three components of its cyber diplomacy in regional and international fora (MOFA, 2019). But the alarming rate and severity of cyberattacks and fraying global consensus on internet governance have forced the Japanese government to rethink its approach and elevate cybersecurity as a core defense and security issue amid the limitations imposed by its pacifist constitution. Japan's increasing defense allocation exemplified by the so-called 'Abe Doctrine' represents the growing trend of military normalization in Japan's defense and security strategy (Akimoto 2018; Dobson 2017; Envall 2020; Hughes 2015). This has set the stage for Japan's cybersecurity outlook to evolve from securitization to militarization (Bartlett 2020; Kallender and Hughes 2017).

To demonstrate its resolve in developing its deterrence capabilities across all domains including cyberspace, Former Prime Minister Shinzo Abe in 2017 raised Japan's military spending beyond the one percent threshold of the country's Gross Domestic Product (Pryor and Le, 2018). By 2020, the defense budget spending plan has reached an all-time high of US$47 billion. Under the 2018 Defense Strategy Japanese cybersecurity spending has doubled from US$100 million to US$235 million between 2018 and 2019. With increased funding, the Japan Cyber Defense Group under the Japan Self-Defense Forces Command, Control, Communication, and Computers (C4) Systems Command is expected to recruit additional personnel from 220 to 290 by the end of March 2021 (Gady and Koshino 2020). The on-going efforts to upgrade JSDF's cyber capabilities are part of the National Defense Program Guidelines and Medium-Term Defense Program (MTDP) published in 2018 that aims to build Japan's Multi-Domain Defense Force. Modelled after the US multi-domain operations, the MTDP aims to synchronize all capabilities in each domain through effective command, control, communications, computers, and information (Gady and Koshino 2020). But it remains unclear how Japan will operationalize the integration of different domains since the Self-

Defense Force Law only allows the establishment of joint operations command or joint task force under very specific and unique circumstances (Gady and Koshino 2020).

The Japan's defense ministry also plans to invest US$237.12 million to develop an Artificial Intelligence-enabled system to deter cyberattacks (DefenseWorld 2020b). The Ministry of Defense (MOD) plans to deploy AI in communications networks of the JSDF counter cyberattack unit starting in 2020 to detect and neutralize viruses and malware and predict future threats (Rieki 2019). Using AI-enabled cyber tools, MOD also aims to build a Cyber Information Gathering System amounting to US$31.5 million to gather critical information on the tactics, techniques, and procedures (TTPs) used by threat actors against the JSDF and identify potential irregular activities on the network devices of the Japanese military (Defense World, 2020a). MOD has also committed to improving the Defense Information Infrastructure and the Controllability and Situation Awareness of System Network (Akimoto 2020). For the very first time, Japan also led the joint international digital defense exercise with over 20 countries, including the US, UK, France, and ASEAN (Tajima 2020). The digital defense exercise held in the latter part of 2020 tackled the salience of hacking and disinformation campaigns in light of the US elections, and the global pandemic (Tajima 2020).

The deepening uncertainty in the cyber landscape driven primarily by China, alongside North Korea, Russia and compounded by Trump's persistent call on alliance burden-sharing have rapidly accelerated Japan's tight grip in developing its defensive posture in cyberspace. Japan's militarized response in cyberspace depicts more broadly its 'security renaissance' (Oros 2017). But due to the limitations posed by its Post-World War II constitution, Japan may develop capabilities but purely for defensive purposes (Bartlett 2020). In effect, Japan's rising defensive capabilities will demand a realignment within the broader framework of CBMs in cyber diplomacy. As stated in the *2018 Cybersecurity Strategy*, Japan will utilize CBMs to mitigate any misinterpretation of its deterrence capability. The overall goal is to build trust among international actors to prevent the 'occurrence of unforeseen circumstances and deterioration of the situation caused by cyberattacks' (Vose 2019, 19). Japan's improved cyber defense posturing is thus complemented by the reinvigoration of its CBMs as a form of preventive diplomacy. CBMs are instrumental for Japan to prevent any danger of miscalculation or misunderstanding towards its emerging defensive outlook in cyberspace.

With its increasing emphasis on the application of deterrence in the cyber domain, Japan has consistently invoked its constitutional and international obligations on the acceptable use of force to foster a level of mutual understanding and mitigate any fear or doubt. Former Prime Minister Shinzo Abe stated that 'under the Constitution, Japan will be allowed to exercise force for self-defense' but under very specific conditions (Mainichi 2019). Japan's longest-serving premier argued that responding to cyberattacks 'should be judged on a case-by-case basis based on factors such as international circumstances, the other party's explicit intention, the means employed in the attacks, and responses to them' (Mainichi 2019). Adding more clarity on what constitutes an armed attack, Abe suggested that such incidents are defined as 'cases in which extremely serious damage on par with that caused by attacks by physical means arises, and the attacks are made by the other party in a systematic and premeditated manner' (Mainichi 2019).

Similarly, according to Daisuke Akimoto, Director of Economic Security Policy Division of the Ministry of Foreign Affairs, Japan's use of force in cyberspace is justified under international law on the use of force and the laws of armed conflict. During Japan's chairmanship of the G7 Summit in 2016, it advocated for the *Ise-Shima* principles and actions on cyber which underscored that 'under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of international law (MOFA 2016a). The use of force is considered legal in international conflict resolution as mandated by the United Nations Charter but the right to exercise individual and collective-self defense must first satisfy a level of 'necessity' and 'proportionality' (MOFA, 2016b). Despite the restrictions of Article 9 in the Japanese constitution to use force in settling international disputes, the Abe government has confirmed that Japan has the right to self-defense and the right to exercise individual and collective self-defense according to the three provisions outlined in the Peace and Security legislation: (1) When an armed attack against Japan occurs and as a result threatens Japan's survival and poses a clear danger to fundamentally overturn people's right to live, liberty, and pursuit of happiness, (2) When there is no other appropriate means available to repel the attack and ensure Japan's survival and protects its people, (3) Use of force limited to the minimum extent necessary (MOFA, 2016). Akimoto (2020) posits that the three conditions enshrined in the Peace and Security legislation are consistent with the criteria stipulated on the use of force in line with international law 'given the nature of cybersecurity in modern military and operations and tactics'. This led Akimoto (2020) to conclude that 'Japan's right to exercise individual and collective self-defense can be justifiable in light of the Japanese Constitution and international law'. Mindful of the possible political repercussions of its defense-oriented cyber policy, the Japanese government threads a delicate balance of achieving a deterrent effect while facilitating greater transparency and information. On one hand, it acknowledges the rapid build-up of its defensive cyber capabilities but also emphasizes its right to self-defense within the remit of international law.

When it comes to public attribution, Japan has taken a more measured approach. In 2017, it has joined the Five Eyes Community to denounce North Korea as the perpetrator of WannaCry (Raj 2017). Japan also named and shamed Chinese-linked APT10 alongside the US, and the UK to demonstrate its resolve to uphold its commitment to the prohibition of using ICT-enabled theft of intellectual property. However, it did not join the same group in naming or shaming Russian hackers behind NotPetya. In an interview with a few cybersecurity experts in Japan, they argue that the government has been prudent in using the naming and shaming tactic to avoid any diplomatic fallout. This explains why Japan joined the Five Eyes against North Korea while opting out when Russia was involved due to their on-going negotiations on territorial issues in the Northern part of Japan. Japan's use of the attribution card also shows its strong preference towards a concerted effort rather than conducting it independently to cushion a potential diplomatic downturn. Even with the increasing use of public attribution by the US, UK, and Australia, Japanese cyber policy experts argue that the Japanese government will remain circumspect in using the public attribution card within its overall cyber strategy.

Deterrence is also a key driver in shaping Japan's unique approach to capacity-building engagement in Southeast Asia. Through its Overseas Development Assistance, Japan conducts its cybersecurity capacity building which contributes to its defense and foreign

policy interests, primarily aimed at countering China's influence in the Asia Pacific (Potter 2015, 56). Japan's *2018 Cyber Strategy* highlighted three critical areas where Japan can take a leading role: (1) International Cooperation and Collaboration, (2) Incident Response and; (3) Capacity Building.

Under the 2016 Basic Policy to Cybersecurity Capacity Building for Developing Countries, the Japanese government has been engaged in establishing emergency response teams (CERTs); cooperating with law enforcement on cybercrime, and; setting the agenda for international norms and values and confidence-building through the UN GGE (Matsubara 2017). Japanese companies are also being encouraged to contribute to improving the cybersecurity in other countries based on the said policy (Vose 2019). ASEAN is a strategic focus for Japan's regional capacity-building in the realm of technical-training and norm-setting. Japan and ASEAN have established various diplomatic platforms to promote capacity-building initiatives which include the ASEAN-Japan Information Security Policy Meeting, the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation, ASEAN-Japan Ministerial Meeting (AMMTC + Japan), and the Senior Officials Meeting on Transnational Crime (SOMTC + Japan) (Vose 2019).

Japan's capacity-building initiatives have grown throughout the years, from a policy to technical type of capacity-building assistance. During the very first Informational Security Policy Meeting in 2009, the agenda revolved around crafting cybersecurity strategies and sharing best practices. But as ASEAN member states gradually developed their CERTs, Japan's capacity initiatives shifted to improving their national cybersecurity capability (Matsubara 2017). In commemoration of the 40th anniversary of the Japan-ASEAN relationship in 2013, the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation launched the Internet Traffic Monitoring Data Sharing Project (TSUBAME). The project aims to expand the threat-information sharing cooperation between Japan Computer Emergency Team/Coordination Center (JPCERT/CC) and other CERTS in the Asia Pacific region to monitor malicious internet traffic (Matsubara 2017). Japan and ASEAN have also vouched to exchange technical know-how in the cooperation of Internet Service Providers. To further enhance technical cooperation, the Japan-ASEAN Security Partnership (JASPER) was also established which will facilitate the Proactive Response Against Cyberattacks Through Collaborative Exchange (PRACTICE) project and infection alerting (MIC, 2013). Issues relating to cyberattacks that endanger critical national infrastructure have also received traction among ASEAN member states and Japan. In 2016, ASEAN countries have subscribed to Japan's national critical information infrastructure policy in drafting their cybersecurity guidelines to protect their electric power industry and set up an emergency liaison system to ensure business continuity (METI, 2016).

Japan took its capacity-building engagement in ASEAN a step further when it formally established the ASEAN-Japan Cybersecurity Capacity Building Center (AJCCBC) in Thailand in 2018. AJCCBC will play a key role in augmenting ASEAN's deterrence posture through the establishment of region-wide CERT with a dedicated pool of cybersecurity workforce (Bhunia 2018). The centre will offer three courses on Cyber Defense Exercise with Recurrence for cybersecurity incidents; Forensics analysis for digital evidence and Malware analysis (Bhunia 2018).

Australia

The *International Cyber Engagement Strategy* released in 2016 enshrines Australia's Cyber Diplomacy. According to the Department of Foreign Affairs and Trade (DFAT), the document advocates for a whole of government approach, using the full-spectrum of Australian diplomatic tools and resources to achieve its overarching goal of creating a stable and peaceful online environment. Under DFAT's leadership, Australia's international cyber diplomacy rested on three objectives: (1) Deterring and responding to unacceptable behaviour in cyberspace; (2) Implementing practical confidence-building measures and; (3) Setting clear expectations for state behaviour in cyberspace.

Through the *2019 Progress Report* on its cyber diplomacy, the Australian government has conducted its first comprehensive review of response options against 'unacceptable behaviors' in cyberspace ranging from diplomatic, economic, legal, and law enforcement (DFAT 2019). But a critical touchstone to Australia's cyber diplomacy includes its loud emphasis on the possible use of offensive and defensive cyber capabilities to deter growing cyber threats. Former Prime Minister Malcolm Turnbull (2017) did not shy away in publicly declaring Australia's possession of such military capability during the launch of Australia's *2016 Cyber Security Strategy*. Turnbull (2017) stated that Australia has invested A$230 million to support the implementation of its National Cyber Security Strategy, while the Defense White Paper disclosed funding worth A$400 million allocated to upgrade the defense forces' cyber capabilities.

The offensive cyber capabilities are housed in the Australia Signals Directorate (ASD) and cyber operations are conducted largely by civilians that act within the laws of armed conflict and legally approved instructions (Hanson and Uren 2018, 6). Offensive cyber operations in support of the Australian Defense Force (ADF) are conducted by the ASD with the Joint Operations Command under the direction of the Chief of Joint Operations (Hanson and Uren 2018, 6). The use of offensive cyber capabilities is executed similarly to the kinetic ADF operations (Hanson and Uren 2018, 7). All offensive cyber operations are directed by the Chief of Joint Operations and governed by the ADF rules of engagements, making Australia's offensive cyber capabilities a joint civil–military partnership (2018, 7). Hanson and Uren (2018, 7) contend that 'the full integration of Australia's military offensive cyber capability with ADF operations sets Australia's capability apart from that of many other countries'. They argue that the civil–military fusion affords Australia with asymmetric capabilities within a wide range of contexts as seen during the coalition operations in Iraq and Syria (Hanson and Uren 2018, 8).

However, Turnbull is quick to clarify that 'the use of cyber capability is subject to stringent legal oversight and is consistent with our support for the international rules-based order and our obligations under international law' (Karp 2021). The use of cyber capabilities is governed by four core principles—Necessity, Specificity, Proportionality, and Harm—and subject to ASD's legislative and oversight framework, including the independent oversight by the Inspector-general of Intelligence and Security (Hanson and Uren 2018, 8–9). Turnbull contends that his public revelation on Australia's cyber capability provides a 'level of deterrence' and builds its international reputation as 'it adds to our credibility as we promote norms of good behavior … and importantly [the] familiarity with offensive measures enhances our defensive capabilities as well' (Karp 2021).

The current Morrison government has not only sustained its predecessor's efforts but even elevated Australia's deterrence posture in cyberspace. After releasing a statement about the overwhelming cyber hacking from a 'state-sponsored actor'—which was later on leaked to the press as China—the Australian government made an avalanche of cyber policy initiates (Cave, Uren, and Kang 2020). The '(un)naming and shaming' of China's alleged massive intrusions was used as a pretext to launch Australia's *2020 Cyber Strategy*, as well as the International Cyber Engagement Strategy and Critical Technology. It was observed that the build-up to Australia's 2020 cyber strategy emblematically represents the document's sharper edge on deterrence, stating that '[Australia] work [s] to actively prevent cyberattacks, minimize damage, and respond to malicious cyber activity directed against our national interests. We deny and deter, while balancing the risk of escalation. Our actions are lawful and aligned with the values we seek to uphold, and will therefore be proportionate, always contextual and collaborative. We can choose not to respond'.

Following the release of the cyber strategy, Australia unveiled its latest cyber investment called the Cyber Enhanced Situational Awareness and Response package amounting to $930 million (Austin 2020). The package will bolster ASD's cybersecurity workforce with an additional 1700 new personnel, while the ADF will also boost its joint-cyber unit with additional 900 recruits (Austin 2020). The release of the 2020 Cyber Strategy reignited debates about Australia's rapid transition into offensive posturing in cyberspace (Duckett 2020). The Federal government will use its offensive capabilities to defend its networks as well as the potential adoption of an 'active cyber defense' for low-level cyber threats (StillgHerrian 2020). Furthermore, the ASD also gains additional powers to obtain access to the networks and data of companies operating critical national infrastructures in real-time, raising serious concerns from the private sector (Galloway 2020).

The Australian government has also upped the ante by using public attribution to deter malicious behaviour online. According to DFAT's *2019 Progress Report*, since 2017 Australia has been 'forward-leaning in calling out unacceptable behavior'. Australia's notable 'naming and shaming' campaign included the collective public attribution campaign against WannaCry perpetrated by North Korea in 2017 and 'NotPetya' to Russian state-sponsored actors in 2018. Australia joined various initiatives to condemn Russian cyber operations in 2018. This includes a joint statement with the US and UK about Russia's global targeting of Cisco routers; 21 international partners notifying Russian cyber activity against political institutions, businesses, media, and sport and; Russia's involvement in the MH17 investigation. In the same year, Australia has also called out APT10, a Chinese-linked hacking group involved in global intellectual property theft operations.

Capacity-building efforts are also central to Australia's international cyber engagement geared towards improving the deterrence capacity of neighbouring Pacific Island nation-states, and ASEAN. Through its Cyber Cooperation Program, DFAT has been pursuing a two-pronged approach of promoting the soft dimensions of its cyber diplomacy while investing in the technical capacity building in the region to deter transnational cyber threats. For instance, Australia has been providing assistance to ASEAN member states and Pacific islands to institutionalize technical capabilities and cybersecurity awareness as well as the promotion of norms and international law. Additionally,

it has also strengthened the local cybersecurity capacity and technical foundation for the establishment of the National Computer Emergency Response Team (CERT) in the Pacific. Under the same programme, Australia supported the Asia Pacific Network Information Center to further boost regional cybersecurity capacity. It has also institutionalized the technical capability development of CERTs in Tonga and Vanuatu and the creation of the Security Operations Center in the Solomon Islands. With Australia's support, Samoa also produced its handbook for the ICT sector to espouse best-practices tailored to local needs. After laying the groundwork for technical capacities at the local and country-level, Australia has set up the Pacific Cyber Security Operational Network (PACSON) for threat-information sharing and sustain the existing technical capacity building in April 2018.

Compared to the Pacific Islands, Australia's engagement with ASEAN has favoured more assistance towards the promotion of international law and norms and the development of CBMs. Based on *the 2019 Progress Report*, DFAT co-sponsored the Australia-ASEAN Cyber Risk Reduction workshop in 2017 that dived into international law as well as scenario planning and crisis management. In July 2018, through the Cyber Cooperation Program, Australia convened a workshop with ASEAN member states on the application of international law in cyberspace. Australia has utilized the ASEAN Regional Forum (ARF) to develop a framework for a point of contact directory to facilitate connectivity and communication among ARF participants in the event of cyber incidents that are regional in scale. Aside from the ARF, Australia had also utilized the ASEAN Defense Minister's Meeting-Plus Experts Working Group to clarify cyber terminologies along with escalation and communication channels and procedures. According to a DFAT foreign officer, all of Australia's CBM efforts fall under its objective to foster transparency on the limits of its cyber capabilities by emphasizing its commitment to international cyber norms.

Further strengthening regional cyber cooperation, the Turnbull government held the first-ever ASEAN-Australia Special Summit in 2018 that demonstrated Australia's commitment to cybersecurity and international terrorism (Othman 2018). Turnbull emphasized the rising salience of cyber terrorism and the need to apply laws both offline and online (Othman 2018). To support the summit, DFAT released the *Sydney recommendations on Practical Futures for Cyber Confidence Building* in ASEAN which convened a region-wide group of experts from think tanks, industry, and academia to tackle concrete steps on confidence and capacity-building in cyberspace (Australian Strategic Policy Institute 2018). Reaffirming Australia and ASEAN's commitment towards a peaceful and stable online environment, the set of policy recommendations called for intragovernmental and multi-stakeholder approach in the region, while espousing for increased CERT cooperation, the establishment of a Track 2 community and industry partnerships (Australian Strategic Policy Institute 2018).

Conclusion

The study has demonstrated that Japan and Australia adhere to the foundational precepts of the cyber diplomacy framework but observed practice unveiled an increasing trend to integrating deterrence in the equation. Understanding Japan and Australia's relative positionality as middle powers or second-tier states from a network perspective,

explicated the rationale behind such recalibration in their cyber diplomacy playbook as they borrow elements from the defense and security policy. The compounding effects of China's aggressive cyber operations and the US potential disengagement set against the backdrop of an evolving and transnational cyber threat landscape, and the impasse in internet governance contributed to the refashioning of Japanese and Australian cyber diplomacy engagements. Throughout its analysis, the article challenged the extant literature on cyber diplomacy that dismisses deterrence. It offered insights as to how the concept of deterrence in cyberspace could be applied, renewing its analytical currency away from its prevailing one-dimensional cold war analogies. Additionally, it also provided a more nuanced understanding on the process of attribution based on technical and political parameters and demystifying the notion of perfect attribution.

However, the article claims that deterrence—cyber capabilities and public attribution—is employed in conjuncture with the fundamental elements of cyber diplomacy—capacity building, CBMS, and cyber norms—to still reinforce the normative and operational precepts in cyberspace to mitigate any escalation or misinterpretation. The deterrent effects of cyber capabilities provides an immediate layer of defense against the instantaneous cyber threats posed by malicious actors. But maintaining stability remains the most paramount goal among nation states' cyber policies. As shown in the Australian case, there is a flow-on effect surrounding cyber capabilities in reinforcing acceptable standards of behaviour in cyberspace. Furthermore, the invocation of cyber capabilities to deter hostile actors are not conducted in silos as illustrated by Japan and Australia. The specific circumstances and the jurisdictions upon which they are employed are outlined and are consistent with international law. In the process, cyber capabilities are complemented by CBMs to ensure predictability and transparency, and to avoid any miscalculation or unwarranted escalation. And despite the emphasis on deterrence especially on the use of strong rhetoric surrounding the deployment of offensive cyber capabilities to deter adversaries, the analysis of the Japanese and Australian cases reveal that the purpose remains largely defensive.

But beyond developing their cyber capabilities, deterrence is also central in the provision of capacity-building activities in Southeast Asia and the Pacific Island nation-states, especially on Japan's use of development aid. With the transboundary nature of cyber threats, providing technical assistance to improve computer emergency response, threat-information sharing, and enhance digital forensic capabilities fortify the region's overall deterrence capabilities, which in return, unequivocally supports Japan and Australia's respective cyber strategies. While the progress on cyber norms and international law remains in limbo, naming and shaming have proven its inherent shaping effects to reinforce what constitutes responsible state behaviour. Although imperfect, the social and reputational damage associated with public attribution puts the onus on the alleged perpetrator to act accordingly based on implied norms and acceptable decorum. The naming and shaming card achieves a deterrent effect, setting in motion the *de jure* application or reinstatement of international law or the possible construction of a new set of norms.

As the ICT landscape continues to morph with technological advancements and innovations, nation-states need to continuously adapt and refine their approaches. The cyber domain is riddled with multiple ambiguous and known actors, possessing competing values and interests, which, produce disruptive effects and emerging practices. The

dynamics of these factors will breed new types of opportunities as well as challenges and risks demanding novel approaches. With the influx of changes and disruptions, the cyber diplomacy playbook will continue to evolve to match the changing cyber landscape. In this aspect, nation-states must possess a high degree of flexibility and agility to navigate the shifting sands of international cyber (in)security. As the article has shown, there is a growing acquiescence between Japan and Australia which they can explore further in their cyber dialogue. As both countries aim to expand their cyber diplomacy on other areas such as critical and emerging technology, regional and global supply chains, tech and data governance, greater policy coordination and resource allocation management are imperative to generate a positive-net impact that will benefit the entire Asia Pacific region.

Note

1. For example, the US Cyber Policy Review (2009), International Strategy for Cyberspace (2011) and National Cyber Engagement Strategy (2018) sit alongside China's White Paper for the Internet (2010), Japan's International Strategy on Cybersecurity Cooperation (2013), Australia's International Cyber Engagement Strategy (2017); and the ASEAN Cyber-security Cooperation Strategy (2017). See complete or updated list at: https://unidir.org/cpp/en/.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This work was supported by Pacific Forum under the Lloyd and Lilian Vasey Fellowship.

Notes on contributor

Mark Bryan F. Manantan is currently the Lloyd and Lilian Vasey fellow at the Pacific Forum and concurrently, a non-resident fellow at the Center Southeast Asian Studies at the National Chengchi University in Taiwan. Recently he was based at the Center for Rule-making Strategies at Tama University in Tokyo, Japan, and East-West Center in Washington DC as a 2020 US-Japan-Southeast Asia Partnership in a Dynamic Asia Fellow.

ORCID

Mark Bryan F. Manantan http://orcid.org/0000-0001-9287-4191

References

2020a. "Japan to Develop AI-based System to Counter Cyber Attacks." *Defense World*, March 30. Accessed September 10, 2020. https://www.defenseworld.net/news/26616/Japan_to_Develop_AI_based_System_to_Countetr_Cyber_Attacks#.X2m2IZMzZfU.

2020b. "Japan to Develop AI-Based System to Counter Cyber Attacks." *DefenseWorld*. Accessed March 13, 2020. https://www.defenseworld.net/news/26616/Japan_to_Develop_AI_based_System_to_Counter_Cyber_Attacks.

Akimoto, Daisuke. 2018. "Introduction." In *The Abe Doctrine: Japan's Proactive Pacifism and Security Strategy*, edited by Daisuke Akimoto, 1–8. Singapore: Springer. doi:10.1007/978-981-10-7659-6_1.

Akimoto, Daisuke. 2020. "Cybersecurity and Japan's Right to Self-Defense." *ISDP*, June 11. Accessed September 10, 2020. https://isdp.eu/cybersecurity-japans-right-to-self-defense/#:~:text=On%20May%2016%2C%202019%2C%20Prime,armed%20attacks%20on%20Japan%20occur.

Austin, Greg. 2020. "Morrison's $1.3 Billion for More Cyberspies is an Incremental Response to a Radical Problem." *The Conversation*, June 30. Accessed September 4, 2020. https://theconversation.com/morrisons-1-3-billion-for-more-cyber-spies-is-an-incremental-response-to-a-radical-problem-141692.

Australian Strategic Policy Institute. 2018. "Sydney Recommendations on Practical Futures for Cyber Confidence Building in the ASEAN Region." *Australia-ASEAN Council*, September. Accessed September 8, 2020. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-09/Sydney%20recommendations_Cyber-ASEAN.pdf?kwrNP4FHCYxE9oGVhxzchUvF3rx11hoG.

Barrinha, Andre, and Thomas Renard. 2017. "Cyber-diplomacy: The Making of an International Society in the Digital Age." *Global Affairs* 3 (4-5): 353–364. doi:10.1080/23340460.2017.1414924.

Barrinha, André, and Thomas Renard. 2020. "Power and Diplomacy in the Post-Liberal Cyberspace." *International Affairs* 96 (3): 749–766. doi:10.1093/ia/iiz274.

Bartlett, Benjamin. 2020. "Japan: An Exclusively Defense-Oriented Cyber Policy." *Asia Policy* 27 (2): 93–100. doi:10.1353/asp.2020.0013.

Belot, Henry. 2017. "Cyber Security 'The New Frontier of Warfare, Espionage', Malcolm Turnbull Says." *ABC News*. Accessed March 9, 2021. https://www.abc.net.au/news/2017-01-24/turnbull-declares-cyber-security-the-new-frontier-of-warfare/8207494.

Betz, David, and Tim Stevens. 2011. "Chapter One: Power and Cyberspace." *Adelphi Series* 51 (424): 35–54. doi:10.1080/19445571.2011.636954.

Bhunia, Priyankar. 2018. "ASEAN-Japan Cybersecurity Capacity Building Center to be launched in Thailand in June 2018." *Open Gov Asia*, March 31. Accessed September 3, 2020. https://opengovasia.com/asean-japan-cybersecurity-capacity-building-centre-to-be-launched-in-thailand-in-june-2018/.

Borghard, Erica D., and Shawn W. Lonergan. 2018. "Confidence Building Measures for the Cyber Domain." *Strategic Studies Quarterly* 12 (3): 10–49.

Brew, Nigel. 2019. "Foreign Interference—Neither New Nor Limited to China." *Parliament of Australia*. Accessed March 9. https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2019/September/Foreign_interference.

Calderaro, Andrea, and Anthony J. S. Craig. 2020. "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building." *Third World Quarterly* 41 (6): 917–938. doi:10.1080/01436597.2020.1729729.

Cave, Danielle, Tom Uren, and Jocelinn Kang. 2020. "What, Who and Why: Explaining the Cyberattacks against Australia." *Australian Strategic Policy Institute*, June 25. Accessed September 9, 2020. https://www.aspistrategist.org.au/what-who-and-why-explaining-the-cyberattacks-against-australia/.

Chua, Joseph B. 2017. "2015 U.S.-China Cyber Agreement: A New Hope, Or the Empire Strikes Back." *Naval Postgraduate School Monterey United States*. https://apps.dtic.mil/sti/citations/AD1053136.

Clarke, Richard A. 2016. "The Risk of Cyber War and Cyber Terrorism." *Journal of International Affairs* 70 (1): 179–181. Accessed March 13, 2021. https://www.jstor.org/stable/90012602.

Cyber Affairs. 2019. "Australia-Japan Cyber Policy Dialogue 2019 Joint Statement." *DFAT*. Accessed August 10, 2020. https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australia-japan-cyber-policy-dialogue-2019-joint-statement.

Deibert, Ron. 2012. "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace." *Journal of Military and Strategic Studies* 14 (2): 1–23. Accessed March 9, 2021. https://jmss.org/article/view/58030.

DFAT 2019 "Progress Report." Accessed September 6, 2020. https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_progress_report.html.
Dobson, Hugo. 2017. "Is Japan Really Back? The 'Abe Doctrine' and Global Governance." *Journal of Contemporary Asia* 47 (2): 199–224. doi:10.1080/00472336.2016.1257044.
Duckett, Chris. 2020. "New Australian Cybersecurity Strategy Will See Canberra Get Offensive." *ZDNet*, August 6. Accessed September 5, 2020. https://www.zdnet.com/article/new-australian-cyber-security-strategy-will-see-canberra-get-offensive/.
Dutton, William H., Sadie Creese, Ruth Shillair, and Maria Bada. 2019. "Cybersecurity Capacity: Does it Matter?" *Journal of Information Policy* 9: 280–306. doi:10.5325/jinfopoli.9.2019.0280.
Egloff, Florian J. 2020. "Public Attribution of Cyber Intrusions." *Journal of Cybersecurity* 6 (1): tyaa012. doi:10.1093/cybsec/tyaa012.
Envall, H. D. P. 2020. "The 'Abe Doctrine': Japan's New Regional Realism." *International Relations of the Asia-Pacific* 20 (1): 31–59. doi:10.1093/irap/lcy014.
Finnemore, Martha, and Duncan Hollis. 2017. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110 (3): 425–479. doi:10.1017/S0002930000016894.
Finnemore, Martha, and Duncan B. Hollis. 2020. "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity." *European Journal of International Law* 31 (3): 969–1003. doi:10.1093/ejil/chaa056.
Fischerkeller, Michael P., and Richard J. Harknett. 2017. "Deterrence is not a Credible Strategy for Cyberspace." *Orbis* 61 (3): 381–393. doi:10.1016/j.orbis.2017.05.003.
Francis, David. 2015. "Obama Slams North Korea With Sanctions for Sony Hack." *Foreign Policy*, January 2. Accessed September 8. https://foreignpolicy.com/2015/01/02/obama-slams-north-korea-with-sanctions-for-sony-hack/.
Gady, Franz-Stefan. 2017. "Japan: The Reluctant Cyberpower." *French Institute of International Relations*. Accessed March 2, 2020. https://www.ifri.org/en/publications/notes-de-lifri/asie-visions/japan-reluctant-cyberpower.
Gady, Franz Stefan, and Greg Austin. 2010. "Russia, The United States, and Cyber Diplomacy Opening Doors." *East West*, September 14. Accessed August 31, 2020. Institute. https://www.eastwest.ngo/idea/russia-united-states-and-cyber-diplomacy-opening-doors.
Gady, Franz-Stefan, and Yuka Koshino. 2020. "Japan and Cyber Capabilities: How Much is Enough?" *IISS*, August 28. Accessed September 1, 2020. https://www.iiss.org/blogs/military-balance/2020/08/japan-cyber-capabilities.
Galloway, Anthony. 2020. "Cyber Spy Agency to be Called in to Protect Critical Infrastructure." *SMH*, August 6. Accessed September 1, 2020. https://www.smh.com.au/politics/federal/cyber-spy-agency-to-be-called-in-to-protect-critical-infrastructure-20200806-p55j6m.html.
Geist, Edward. 2015. "Deterrence Stability in the Cyber Age." *Strategic Studies Quarterly* 9. https://fsi.stanford.edu/publication/deterrence-stability-cyber-age.
Goodman, Will. 2010. "Cyber Deterrence: Tougher in Theory Than in Practice?" *Strategic Studies Quarterly* 4 (3): 102–135. https://www.jstor.org/stable/pdf/26269789.pdf?refreqid=excelsior%3Af112c3384ab1093b18057eac322ae862.
Grigsby, Alex. 2017. "The End of Cyber Norms." *Survival* 59 (6): 109–122. doi:10.1080/00396338.2017.1399730.
Hamilton, Clive. 2021. "How Australia is Fighting Chinese Political Interference." *Foreign Affairs*. Accessed March 9. https://www.foreignaffairs.com/articles/australia/2018-07-26/australias-fight-against-chinese-political-interference.
Hanson, Fergus, and Tom Uren. 2018. *Australia's Offensive Cyber Capability*. Canberra: Australian Strategic Policy Institute. Accessed September 4, 2020. https://www.aspi.org.au/report/australias-offensive-cyber-capability.
Heazle, Michael, and Yuki Tatsumi. 2018. "Explaining Australia–Japan Security Cooperation and its Prospects: 'The Interests that Bind?" *The Pacific Review* 31 (1): 38–56. doi:10.1080/09512748.2017.1310750.
Henriksen, Anders. 2018. "The end of the Road for the UN GGE Process: The Future Regulation of Cyberspace." *Journal of Cybersecurity* 5 (1): 1–9. doi:10.1093/cybsec/tyy009.

Hill, Jonah Force. 2012. "A Balkanized Internet?: The Uncertain Future of Global Internet Standards." *Georgetown Journal of International Affairs* 2012: 49–58. Accessed March 9, 2021. http://www.jstor.org/stable/43134338.

Hocking, Brian, Jan Melissen, Shaun Riordan, and Paul Sharp. 2012. "Futures for Diplomacy." *Clingendael* 1. Accessed September 3, 2020. https://www.clingendael.org/sites/default/files/pdfs/20121030_research_melissen.pdf.

Hoffmann, Stacie, Dominique Lazanski, and Emily Taylor. 2020. "Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet." *Journal of Cyber Policy* 5 (2): 239–264. doi:10.1080/23738871.2020.1805482.

Hughes, C. 2015. *Japan's Foreign and Security Policy Under the 'Abe Doctrine': New Dynamism or New Dead End?* New York: Palgrave MacMillan.

Hurel, Louise Marie, and Luisa Cruz Lobato. 2018. "Unpacking Cybernorms: Private Companies as Norm Entrepreneurs." *Journal of Cyber Policy* 3 (1): 1–4. doi:10.1080/23738871.2018.1467942.

Iasiello, Emilio. 2014. "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security* 7 (1): 54–67. doi:10.5038/1944-0472.7.1.5.

Iasiello, Emilio. 2016. "China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities." *Journal of Strategic Security* 9 (2): 45–69. https://www.jstor.org/stable/26466776.

Jensen, Eric Talbot. 2012. "Cyber Deterrence." *Emory International Law Review* 26: 773–824. https://law.emory.edu/eilr/_documents/volumes/26/2/symposium/jensen.pdf.

Kallender, Paul, and Christopher W. Hughes. 2017. "Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace." *Journal of Strategic Studies* 40 (1–2): 118–145. doi:10.1080/01402390.2016.1233493.

Karp, Paul. 2021. "Malcolm Turnbull Reveals Cyber-Attacks Breached Government Agencies." *The Guardian*, April 21. Accessed September 8, 2020. https://www.theguardian.com/technology/2016/apr/21/malcolm-turnbull-reveals-cyber-attacks-breached-agencies.

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven; London: Yale University Press. Accessed March 9, 2021. http://www.jstor.org/stable/j.ctt1trkjd1.

Kennedy, Andrew B., and Darren J. Lim. 2018. "The Innovation Imperative: Technology and US–China Rivalry in the Twenty-First Century." *International Affairs* 94 (3): 553–572. doi:10.1093/ia/iiy044.

Kim, Sangbae. 2014. "Cyber Security and Middle Power Diplomacy." *The Korean Journal of International Studies* 12: 323–352. doi:10.14731/kjis.2014.12.12.2.323.

Kleiner, Juergen. 2008. "The Inertia of Diplomacy." *Diplomacy & Statecraft* 19 (2): 321–349. doi:10.1080/09592290802096380.

Knopf, Jeffrey. 2013. "Use With Caution: The Value and Limits of Deterrence Against Asymmetric Threats." *World Politics Review*. Accessed March 9. https://www.worldpoliticsreview.com/articles/13006/use-with-caution-the-value-and-limits-of-deterrence-against-asymmetric-threats.

Lan, Tang, Zhang Xin, Harry Raduege Jr, Dmitry Grigoriev, Pavan Duggal, and Stein Schjølberg. 2010. *Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway*. EastWest Institute: New York.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/monographs/MG877.html.

Liff, Adam P. 2019. "Unambivalent Alignment: Japan's China Strategy, the US Alliance, and the 'Hedging' Fallacy." *International Relations of the Asia-Pacific* 19 (3): 453–491. doi:10.1093/irap/lcz015.

Limnell, James. 2016. "The Cyber Arms Race is Accelerating-What are the Consequences?" *Journal of Cyber Policy* 1 (1): 50–60. doi:10.1080/23738871.2016.1158304.

Lindsay, Jon R. 2015. "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack." *Journal of Cybersecurity*. doi:10.1093/cybsec/tyv003.

Liu, Tao, and Wing Thye Woo. 2018. "Understanding the U.S.-China Trade War." *China Economic Journal* 11 (3): 319–340. https://doi.org/10.1080/17538963.2018.1516256.

Lupovici, Amir. 2011. "Cyber Warfare and Deterrence: Trends and Challenges in Research." *Military and Strategic Affairs* 3 (3). Accessed March 9. http://www.inss.org.il/publication/cyber-warfare-and-deterrence-trends-and-challenges-in-research/.

Mainichi. 2019. "PM Abe Says Japan Can Use Force for Self-Defense against Cyberattacks." *The Mainichi*, May 17. Accessed September 4, 2020. https://mainichi.jp/english/articles/20190517/p2a/00m/0na/002000c.

Manantan, Mark Bryan. 2020a. "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea." *Issues & Studies* 56 (03): 2040013. doi:10.1142/S1013251120400135.

Manantan, Mark Bryan. 2020b. "Prospects for the Philippines-Japan-Australia Trilateral Cooperation." In *Towards an Enhanced Strategic Policy in the Philippines*, edited by A. Arugay, and H. Kraft. Konrad Adenauer Stiftung, and UP Center for Integrative Studies.

Matsubara, Mihoko. 2017. "How Japan is Addressing Cybersecurity Awareness and Capacity-Building Challenges in ASEAN." *Security Roundtable*, July 26. Accessed July 6, 2020. https://www.securityroundtable.org/how-japan-is-addressing-cybersecurity-awareness-and-capacity-building-challenges-in-asean/.

Maurer, Tim. 2020. "A Dose of Realism: The Contestation and Politics of Cyber Norms." *Hague Journal on the Rule of Law* 12 (2): 283–305. https://doi.org/10.1007/s40803-019-00129-8.

Mazanec, Brian M. 2016. "Constraining Norms for Cyber Warfare Are Unlikely." *Georgetown Journal of International Affairs* 17 (3): 100–109. doi:10.1353/gia.2016.0040.

Meer van der, Sico. 2015. "Enhancing International Cyber Security." *Security and Human Rights* 26: 193–205. https://www.clingendael.org/publication/enhancing-international-cyber-security-key-role-diplomacy.

Meer van der, Sico. 2016. "Defense, Deterrence, and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity." In *Securing Cyberspace. International and Asia Perspectives*, edited by Cherian Samuel, and Munish Sharma, 95–105. New Delhi: Pentagon Press.

Meyer, Paul. 2011. "Cyber-Security Through Arms Control." *The RUSI Journal* 156 (2): 22–27. doi:10.1080/03071847.2011.576471.

Meyer, Paul. 2012. "Diplomatic Alternatives to Cyber-Warfare." *The RUSI Journal* 157 (1): 14–19. doi:10.1080/03071847.2012.664357.

Meyer, Paul. 2015. "Seizing the Diplomatic Initiative to Control Cyber Conflict." *The Washington Quarterly* 38 (2): 47–61. https://www.tandfonline.com/doi/abs/10.1080/0163660X.2015.1064709.

Miadzvetskaya, Yuliya. 2021. "Between Strategic Autonomy and International Norm-Setting: The EU's Emergent 'Cyber-Sanctions' Regime." *SSRN Scholarly* Paper ID 3640358. Rochester, NY: Social Science Research Network. doi:10.2139/ssrn.3640358.

MIC. 2013. "Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation." Accessed September 3, 2020. https://www.soumu.go.jp/main_content/000249127.pdf.

MOFA.2016a. "G7 Principles and Actions on Cyber." May 27. Accessed September 8, 2020. https://www.mofa.go.jp/files/000160279.pdf.

MOFA. 2016b. "Japan's legislation for Peace and Security." Accessed February 1, 2021. https://www.mofa.go.jp/files/000143304.pdf.

MOFA. 2019. 'Japan's Cyber Diplomacy.' Accessed September 4, 2020. https://www.mofa.go.jp/files/000412327.pdf.

Moret, Erica, and Patryk Pawlak. 2017. European Union Institute for Security Studies. *The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?* LU: Publications Office. https://data.europa.eu/doi/10.2815/399444.

Mueller, Milton. 2017. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Cambridge, UK: Polity. https://www.wiley.com/enus/Will+the+Internet+Fragment%3F%3A+Sovereignty%2C+Globalization+and+Cyberspace-p-9781509501229.

Muller, Lilly Pijinenburg. 2015. "Cybersecurity Capacity Building in Developing Countries: Challenges and Opportunities". *Norwegian Institute of International Affairs*. https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/284124/NUPI+Report+03-15-Muller.pdf?sequence=3.

Noor, Elina. 2015. "Strategic Governance of Cyber Security: Implications for East Asia". In *Navigating ASEAN-Japan Strategic Partnership in East Asia and in Global Governance*. Eds Rizal Sukma and Yoshihide Soeya. Japan Center for International Exchange. https://jcie.org/researchpdfs/ASEAN-Japan/NavChange/9.pdf.

Nye, Joseph. 2010. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Nye, Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3): 44–71. doi:10.1162/ISEC_a_00266.

Oros, Andrew L. 2017. *Japan's Security Renaissance: New Policies and Politics for the Twenty-First Century*. New York: Columbia University Press. Accessed March 13, 2021. doi:10.7312/oros17260.

Othman, Liyanna. 2018. "ASEAN-Australia Special Summit Ends with Commitments on Cybersecurity, Free Trade." *Channel News Asia*, March 18. Accessed September 10, 2020. https://www.channelnewsasia.com/news/asia/asean-australia-special-summit-commitment-cybersecurity-trade-10054114.

Pawalk, Patryk, and Panagiota-Nayia Barmpaliou. 2017. "Politics of Cybersecurity Capacity Building: Conundrum and Opportunity." *Journal of Cyber Policy* 2 (1): 123–144. doi:10.1080/23738871.2017.1294610.

Potter, Evan. 2002. *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*. McGill-Queen's University Press. https://www.jstor.org/stable/j.ctt7zt0w.

Potter, David. 2015. "Japan's Foreign Aid, Human Security, and Traditional Security." *Journal of the Nanzan Academic Society Social Sciences* 8: 45–60. https://core.ac.uk/download/pdf/236163864.pdf.

Pryor, Crystal, and Tom Le. 2018. 'Looking Beyond 1 Percent: Japan's Defense Expenditures.' *The Diplomat*. April 3. https://thediplomat.com/2018/04/looking-beyond-1-percent-japans-security-expenditures/.

Raj, Yahswant. 2017. "US, UK, Japan Others Accuse North Korea of WannaCry Cyberattack." *Hindustan Times*, December 19. Accessed September 4, 2020. https://www.hindustantimes.com/world-news/us-uk-japan-others-accuse-north-korea-of-wannacry-cyberattack/story-PQXCs7I8RxUDni8kWhE33O.html.

Rid, Thomas, and Ben Buchanan. 2014. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38 (1-2): 4–37. doi:10.1080/01402390.2014.977382.

Rieki, Miki. 2019. "Japan Defense Ministry to Beef up Cybersecurity with AI." *Nikkei Asia*, 2021. Accessed March 13. https://asia.nikkei.com/Politics/Japan-defense-ministry-to-beef-up-cybersecurity-with-AI.

Riordan, Shaun. 2019. *Cyber Diplomacy: Managing Security and Governance Online*. Cambridge: Polity.

Segal, Adam. 2017. "Chinese Cyber Diplomacy in a New Era of Uncertainty." *Hoover Institute*. https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.

Segal, Adam, Valeriy Akimenko, Keir Giles, Daniel A Pinkston, James A Lewis, Benjamin Bartlett, Hsini Huang, and Elina Noor. 2020. "The Future of Cybersecurity Across the Asia-Pacific." *Asia Policy* 15 (2): 57–114. https://www.nbr.org/wp-content/uploads/pdfs/publications/ap15-2_cyberrt_apr2020.pdf.

Segal, Adam, Samantha Hoffman, Fergus Hanson, and Tom Uren. 2018. "Hacking for Cash." *Australian Strategic Policy Institute*. https://www.aspi.org.au/report/hacking-cash.

Smith, Sheila, and Charles McClean. 2017. "US-Japan Relations and the Trump Effect." *Comparative Connections* 18 (3): 9–16. http://cc.pacforum.org/2017/01/us-japan-relations-trump-effect/.

Soesanto, Stefan. 2020. "Japan's National Cybersecurity and Defense Posture: Policy and Organizations." *ETH Zurich*. doi:10.3929/ETHZ-B-000437790.

Solomon, Jonathan. 2011. "Cyber Deterrence between Nation-States: Plausible Strategy or a Pipe Dream?" *Homeland Security Digital Library*. Air University (U.S.). Press, January 1. https://www.hsdl.org/?abstract&did=.

Stevens, Tim. 2012. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33 (1): 148–170. doi:10.1080/13523260.2012.659597.
StillGHerian. 2020. "Support Grows for an Australian Active Cyber Defence Program." *ZDNet*, July 23. Accessed September 12, 2020. https://www.zdnet.com/article/support-grows-for-an-australian-active-cyber-defence-program/.
Taddeo, Mariarosaria. 2018. "The Limits of Deterrence Theory in Cyberspace." *Philosophy & Technology* 31 (3): 339–355. doi:10.1007/s13347-017-0290-2.
Tajima, Yukio. 2020. "Japan to Lead First Cyber Defense Drill with ASEAN, US, and Europe." *Nikkei*, August 9. Accessed September 1, 2020. https://asia.nikkei.com/Business/Technology/Japan-to-lead-first-cyber-defense-drill-with-ASEAN-US-and-Europe.
Thompson, Marcus. 2012. "The Cyber Threat to Australia." *Australian Defence Force Journal*, January. https://search.informit.org/doi/abs/10.3316/INFORMIT.476324460879232.
Tor, Uri. 2015. "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies* 40 (1-2): 92–117. Accessed March 9, 2020. https://www.tandfonline.com/doi/abs/10.1080/01402390.2015.1115975.
Tow, William T. 2017. "President Trump and the Implications for the Australia–US Alliance and Australia's Role in Southeast Asia." *Contemporary Southeast Asia: A Journal of International and Strategic Affairs* 39 (1): 50–57.
Turnbull, Malcolm. 2017. "Offensive Cyber Capability to Fight Cyber Criminals." *Media Releases*, June 17. Accessed September 8, 2020. https://www.malcolmturnbull.com.au/media/offensive-cyber-capability-to-fight-cyber-criminals.
UNESCAP. 2020. "Cyber Resilience in the Asia Pacific, A Review of National Cybersecurity Strategies." *United Nations University*, August 20. Accessed December 30, 2020. https://www.unescap.org/resources/cyber-resilience-asia-pacific-review-national-cybersecurity-strategies.
Vose, Wilhelm. 2019. "Japan's Cyber Diplomacy." *EU Cyber Direct*. Accessed March 13. https://eucyberdirect.eu/content_research/japans-cyber-diplomacy/.
Wilner, Alex S. 2020. "US Cyber Deterrence: Practice Guiding Theory." *Journal of Strategic Studies* 43 (2): 245–280. doi:10.1080/01402390.2018.1563779.