Challenges and Opportunities for Cyber Norms in ASEAN

Candice Tran Dai[a]* and Miguel Alberto Gomez[b]

[a]Asia Centre, Paris, France; [b]Centre for Security Studies, ETH, Zurich, Switzerland

Contact Details

Candice Tran Dai: C.TranDai@centreasia.eu

Miguel Alberto Gomez: miguel.gomez@sipo.gess.ethz.ch

Challenges and Opportunities for Cyber Norms in ASEAN

The growing frequency of state-associated cyber attacks have led to calls for the establishment of rules of behaviour in this increasingly relevant domain. While there has been no shortage of such initiatives over the past decade, their respective outcomes have highlighted unique challenges faced by norm entrepreneurs in cyberspace. Questions of contrasting conceptualization of cyberspace and varying threat perceptions have stymied attempts to establish a globally acceptable set of norms that regulate state behaviour. As the Association of South East Asian Nations (ASEAN) continues to invest heavily in this domain, calls for the creation of cyber norms within the region have been made. Yet despite this positive development, this paper illustrates that the unique characteristics of ASEAN pose significant obstacles to the emergence and eventual internalization of cyber norms. In response, this paper argues that success in this endeavour requires initiatives that focus on confidence and capacity building measures to mitigate these constraints. Although the likelihood of common norms across ASEAN remains uncertain, the approach suggested may lead to the emergence of different, yet congruent norms within the bloc.

Keywords: ASEAN, Cyberspace, Norm Theory, Cyber Conflict, Security

Introduction

In 2015, the United Nations Group of Governmental Experts (UN-GGE) proposed norms to regulate state-behaviour in cyberspace. While similar initiatives have been running several years prior, its significance is emphasized by the continued growth of state-associated actions in cyberspace. This trend has not gone unnoticed within the Association of Southeast Asian Nations (ASEAN). During the June 2016 ASEAN Defence Ministers Meeting (ADMM) a proposal for the establishment of an Expert Working Group on Cybersecurity was made. In October of the same year, during the ASEAN Ministerial Meeting on Cybersecurity (AMMC), Dr. Yaacob Ibrahim, the Singaporean Minister for Communications and Information and Minister-in-Charge of Cybersecurity reaffirmed the need for the development of cyber norms that suite the

unique nature of the region in terms of its socio-political environment and treatment of cyberspace. Almost one year later, as exposed in chairman's statement during the second ASEAN ministerial meeting on cybersecurity, *"[AMCC] participants also expressed their support for moving forward discussions on the adoption of basic, operational and voluntary norms of behaviour in ASEAN to guide the use of ICT in a responsible manner […]"*(ASEAN, 2017). Yet despite such optimism, the introduction of cyber norms in ASEAN faces both conceptual and systemic challenges.

Beyond the region, the regulation of actions in cyberspace is subject to challenges emphasized by the recent collapse of the 2017 UN-GGE. Specifically, questions of the domain's nature and its impact on threat perception have been side-lined to reach consensus amongst participating states. As a regional body, ASEAN is not immune from these obstacles.

A cursory review of the concept paper issued by the ADMM-Plus for the establishment of a cybersecurity experts' working group highlights this very same flaw. While its proponents are correct in citing the economic benefits of cyberspace and the implications of threats levelled against it, the document ignores the differences (e.g. economic, infrastructure, etc.) that exists between states. These variations, in turn, influence the perception of both the threats to and benefits of cyberspace that directly influence the emergence and acceptance of norms within the bloc.

With these in mind, the goal of the paper is not to provide a definitive solution for the emergence of ASEAN-specific cyber norms. Instead, it aims to provide readers with a general direction by which the bloc may increase the likelihood of such norms emerging and taking hold. In so doing, the succeeding pages demonstrates that while a bloc-wide set of norms may be desirable in the long run, initial attempts ought to focus on bridging

the perceptive gap that exists between members to allow more congruent norms to take hold.

To expound on the above points, the remainder of the paper is divided as follows. The succeeding section presents the theoretical challenges associated with cyber norms as well as the current realities with regards to the use of the domain in ASEAN. The paper then highlights the fact that despite the pronouncements made by ASEAN, there does not exists a unified conceptualization of cyberspace and its associated threats and argues that bridging this gap is necessary condition for success. The paper concludes by proposing that the challenges faced by ASEAN in the promotion of cyber norms may be addressed through two complementary solution that calls for both confidence and capacity building to facilitate the emergence of a shared conceptualization of cyberspace.

Norms and Cyberspace

Conceptual Challenges

The growth of inter-state exchanges in cyberspace has prompted calls for guiding principles that serve as a basis for state behaviour within the domain. In a joint press conference with Xi Jinping, former United States President Barack Obama emphasized the *"need to work together, and with other nations, to promote international rules of the road for appropriate conduct in cyberspace"* (Obama, 2015). Reflecting this urgency, the United Nations Group of Governmental Experts (UN-GGE) had, that same year, released their report recommending a number of norms, rules, and guidelines outlining appropriate behaviour of states in cyberspace (UN-GGE, 2015). Commonly defined as shared expectations of proper behaviour that affect various aspects of international relations, the promulgation of norms in cyberspace (i.e. cyber norms) continue to face significant

obstacles. The recent failure of the UN-GGE to reach an agreement in 2017 typifies this dilemma (Väljataga, 2017).

Scholars, citing systemic constraints and ideological inconsistency (i.e. similar perception of values), are doubtful of the emergence of globally-accepted cyber norms (Mazanec, 2015). On the other hand, the presence of on-going international and regional initiatives offers the possibility of the eventual cascade and internalization of such (Finnemore, 2016; Nye, 2014).

Success, however, is far from assured. The concept of cyber norms continues to remain underdeveloped given the overemphasis on outcomes rather than the developmental process (Finnemore, 2016). To an extent, this has led to a disjointed collection of norms with varying degrees of maturity as reflected in the existing regime complexes that frame cyber interactions (Nye, 2014). At the heart of this issue, however, is the persistent absence of consensus over what constitutes cyberspace with respect to state interests (Kuehl, 2009). This has led to the situation in which cyber norms are energetically proposed irrespective of the conflicting views that states have towards the domain that these are meant to regulate.

This overemphasis on outcomes traces back to the persistence of the prevailing *cyber revolution thesis*. As the argument goes, with strategic interests becoming increasingly dependent on cyberspace (e.g. the economy), state actors see an opportunity to exert their influence and pursue objectives by threatening their rivals' respective cyberspaces (Maness & Valeriano, 2016). As the effects of aggression in this domain become apparent, states eventually choose to cooperate through the establishment of norms to preserve their interests and to avoid unnecessary escalation (Forsyth Jr & Pope, 2014). Although the logic is sound, it presupposes that the international system enjoys a

uniform view of cyberspace. This presumed homogeneity, however, is both empirically and theoretically unfounded.

Within both academic and policy circles, the conceptualization of cyberspace remains a point of contention. Kuehl, in his attempt to frame it has identified over a dozen different definitions (Kuehl, 2009). Similarly, NATO-CCDCOE lists at least thirty-six (36) competing definitions from both state and non-state actors – with some having two or more parallel definitions (e.g. the United States) (CCDCOE, 2017). Despite the similarities, specifically references to critical infrastructure, no consensus exists. At best, these have surfaced two general conceptions of the domain: an *inclusive* and *exclusive* model[1] (Betz & Stevens, 2011).

The *inclusive* model treats technology as a key component that allows access to cyberspace. The United States, Japan, and Singapore adopt views that reflect this notion. In contrast, the *exclusive* model frames the domain as the space between hardware components wherein social interaction takes place. In some respects, this contends that cyberspace exists within the minds of users. The definitions employed by China and Russia are prime examples of such as will be seen below. The presence of these two is of note as it offers not only differing conceptualizations of cyberspace, but also implies a possible divergence in threat perception – crucial in the eventual formation of cyber norms (Dunn Cavelty, 2013).

As tempting as it may be to issue a blanket statement arguing that the technical nature of cyberspace dictates that all malicious technology-enabled acts are equally threatening, this is a misleading claim. A review of publicly available cyber strategies

[1] This divergence is also reflected in the use of terminology where the former often adopts cyber security while the later employs information security

highlight existing differences in threat perception emerging from contrasting treatments of cyberspace (Luiijf, Besseling, Spoelstra, & De Graaf, 2011). Yet this begs the question as to what causes these variations.

The earliest account forwarded by Hare proposes that state characteristics such as regime type and military power shape an actor's threat perception with respect to cyberspace (Hare, 2010). Hare argues that liberal regimes are inclined to treat technology-enabled malicious activities as possible threats. Incidents such as the deployment of malware or an attempted Distributed Denial-of-Service (DDoS) against critical infrastructure are given priority over others such as website defacement or hacktivism. The rationale being that these states value the availability of cyberspace as a means of enabling economic interests and the free flow of information through cyberspace. In contrast, those with authoritarian regimes view content that challenge the existing narrative propagated by the regime as a threat to its legitimacy. In both cases, variations in the level of military power further alters an actor’s threat perception.

Hare's model is later revised by Rivera who omits military power as a determinant and asserts that regime type alone influences threat perception (Rivera, 2015). In his view, liberal regimes are more likely to treat cyberspace as an enabler of interaction and commerce and requires protection. To an extent, he argues that the domain serves as a platform through which liberal-democratic values are spread. This view is akin to the *inclusive* model introduced above. In contrast, states with authoritarian regimes see in cyberspace a possible source of instability resulting from counter narratives that threaten the legitimacy of the regime. This frames cyberspace as a means to consolidate power through the control of content – its formation and distribution. This, in turn, is reflective of the *exclusive* model.

The above arguments challenge the assumption that norms naturally emerge due to increased dependence on cyberspace. To start with, states do not possess a uniform view of the domain. This, consequently, leads to contrasting threat perceptions that weaken not only the assumption that states would conclude that norms are necessary but also that congruence in state behaviour would be appropriate. Thus, the underlying conditions provide a caustic environment for the emergence of cyber norms. This impasse is demonstrated in previous efforts to push for the acceptance of the International Code of Conduct for Information Security.

Initially drafted by China, Russia, Tajikistan, and Uzbekistan in September 2011, the document aimed to establish the "*rights and responsibilities of states in cyberspace...with the objective of maintaining international stability and security"* (UN, 2011). While the stated purpose remains innocuous and follows the assumption that regulating behaviour in cyberspace is necessary for stability, its specific contents remain controversial and is unlikely to find global acceptance. Most notably, the threat from information weapons as noted below continues to find limited support within the UN, *"Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate* ***information weapons*** *or related technologies"* [Emphasis Added].

This perception of content as a threat diverges from what is referred to as the "Western consensus" that places a premium on the free flow of information in cyberspace with limited government oversight. Even with the omission of the term in the 2015 version, the ambiguity of the phrasing still suggests that this continues to persist in the minds of the proponents, *"Not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security"* (Rõigas, 2015).

Crucial to tracing the source of this disagreement are the respective definitions of cyberspace held by actors in the debate: China, Russia, and the United States. Russia perceives the domain as *"the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which* ***has an effect on individual and social consciousness****, the information infrastructure, and information itself"* [Emphasis Added](CCDCOE, 2017).

China, for its part, treats it as *"The main function of the information space for people to acquire and process data...* ***a new place to communicate with people and activities****, it is the integration of all the world's communications networks, databases and information, forming a "landscape" huge, interconnected, with different ethnic and racial characteristics of the interaction, which is a three-dimensional space."* [Emphasis Added] (CCDCOE, 2017).

The above definitions share the common view that cyberspace is a technical domain that enables the shaping of thoughts that may potentially be of societal significance. When contrasted with these regimes' interest in maintaining power and coupled with the growing importance of content production and dissemination within social movements, it is not beyond imagining that these actors treat platforms such as Twitter and Facebook as potential threats. Moreover, it is unsurprising that this world view would come into conflict with those held United States and others that view cyberspace solely as a technical domain and shuns the practice of information censorship. This concern regarding the promotion of norms that is not aligned with that of the proponents is further reinforced in the above document with calls for certain actors to avoid taking advantage of their dominant position with respect to information technology. This reminds the reader of the Western dominance in content sharing services – the use of which have the potential for destabilizing regimes.

The need to prioritize the regulation of content over other technical considerations is best seen in the actions of China. Despite the fears of Chinese cyber superiority, their actual offensive capabilities have been curtailed by their focus on censorship (Lindsay, 2014). Although elements of the regime have been linked with several high-profile cyber incidents, their infrastructure remains vulnerable as efforts are invested in the development and enforcement of information control.

With respect to the objectives of this paper, it is important to highlight that the above example is by no means an isolated case. ASEAN, given the heterogeneous nature of its membership in terms of regime type and technical capabilities may result in conflicting conceptualizations of cyberspace. Consequently, this facilitates varying threat perceptions that may hinder efforts to establish a set of norms within the region. Keeping this in mind, the remainder of the paper redirects the discussion away from the global initiatives in cyberspace and focuses on ASEAN.

ASEAN and Cyberspace

The Association of Southeast Asian Nations (ASEAN), comprising ten Southeast Asian states[2], is characterized by a high degree of heterogeneity in terms of economic development, which is perfectly reflected in the degree of maturity of the countries in the region in terms of sectoral development of information and communication technologies (ICT), adoption of digital products and services as well as growth of the digital economy. In terms of cyber maturity, the varying intensity of South East Asian states' commitment and political will to engage with cyber policy and security issues, as well as the diverse

[2] Timor Leste has applied to join ASEAN in 2011, the process of Timor-Leste's accession into ASEAN has been ongoing since then.

political regimes of the countries in the region, have brought out a wide disparity as to their approach to cyberspace. For instance, a country with a high degree of cyber maturity like Singapore is prone to push for advancing norms adoption, capacity-building measures and other cyber policy aspects whereas a country like Myanmar which needs to upgrade its overall cyber maturity is more focused on establishing protection measures regarding its national infrastructures. In other words, South East Asian states' commitment to cyber policy issues depends also on their cyber maturity. In this regard, the International Cyber Policy Centre (ICPC) at the Australian Strategic Policy Institute[3] (ASPI) has developed a cyber maturity metric methodology to assess Asia-Pacific states' cyber capabilities. The third edition of the ICPC report on cyber maturity in the Asia-Pacific region shows that, apart from Singapore, which falls in the high-level category, the vast majority of Southeast Asian countries stand around medium levels, Malaysia attaining the upper-medium level and reaching the second place after Singapore, followed by Thailand, which sits just above the average range, and outpacing lower-medium level rankings of Indonesia, the Philippines, Brunei and Vietnam, whereas Laos, Cambodia and Myanmar are closing the list (Feakin, 2016).

While this assessment echoes the prevalent fundamental and structural disparity between Southeast Asian countries, the wider sub-regional perspective indicates that within the framework of ASEAN, Southeast Asian states have been striving to implement

---

[3] The ASPI Cyber Maturity Index is a weighted index that measures the state-level cyber development across five dimensions: governance, financial cyber-crime enforcement, military application, digital economy and business, and social engagement. While other indices exist such as the ITU Global Cybersecurity Index, that of ASPI's was found to be the most appropriate for our purposes.

a common vision of digital adoption and digital transformation. This shared objective was envisioned in the early 2000s and materialized during one of the first major regional initiatives in November 2000 when the governments of the member states signed the e-ASEAN Framework Agreement. It aimed at laying the foundation for the liberalization of trade in ICT products and services, the development of electronic commerce and the strengthening of ICT infrastructure construction within the region. Since then, ASEAN has been consistently working on furthering and deepening what it calls the 'connectivity' of the region (ASEAN, 2011, 2015). This imperative is becoming even more crucial with the official existence of the ASEAN Economic Community of ASEAN (ASEAN Economic Community, AEC) in 31 December 2015. It constitutes an additional step towards the integration project of Southeast Asia and carries with it strong ambitions in the digital domain. From the onset of ASEAN's approach to the digital domain, we may consider that the emphasis has been primarily laid on ensuring the economic development of the region, and consequently the digital economy[4].

There is no doubt at all that Southeast Asia exhibits favourable conditions for the expansion of digital societies and economies and that the region nurtures strong ambition to reach its digital potential. Nevertheless, one of the important key factors in driving digital advancement lies in digital confidence because how much users trust digital products and services can be either a growth enabler or a significant impediment with regards to the digital economy. In the field of information security, protection of personal data and privacy, and more widely cybersecurity, Southeast Asia has only begun recently to tackle those issues more concretely at regional level, whereas at national level the

[4] Consequently, issues concerning cyberspace has predominantly taken an economic tone rather than a political-security orientation.

diversity of strategies and capacities reflects the heterogeneity of the region in approaching and treating the subject. The region has had several wake-up calls in recent years, especially in the field of cyber criminality, hacktivism and cyber espionage, with the occurrence of notable cyber incidents.

Generally speaking, cyber threats do not arise in a vacuum disconnected from political, economic and geopolitical realities; on the contrary, they often constitute a manifestation or an extension of pre-existing tensions and rivalries (Tran Dai, 2014). Cyberspace is therefore a revealing feature of the dynamics at play in the region. In Southeast Asia, three major contextual factors tend to influence the contours of cyberspace, and consequently the evolution of the cyber threats landscape: growing and increasingly digitized economies, the modernization of armies and increase of military spending, territorial disputes that generate renewed geopolitical tensions. The economic vitality of the countries of the region has become very attractive and engenders dedicated cyber threats motivated not only by the lure of gain but also by economic and commercial competition. Several Southeast Asian governments have integrated information and communication technologies into their overall socio-economic development strategy. The rapid development of digital economies and societies in the region has resulted in increased reliance on ICT in terms of economic prosperity. The evolution of military budgets in Southeast Asia shows that the region has experienced steady growth in military spending between 2010 and 2014, with net increases for all countries in the region (Markit, 2017). This heavy trend is reflected in military modernization objectives, which have risen to the top of the political agenda in several countries in the region. Geopolitical rivalries fuel renewed tensions in Southeast Asia, with territorial disputes in the South China Sea concentrating much of the activity of cyber espionage and hacktivism in the region. The cyber dimension of traditional geopolitical conflicts in the region has gained

prominence in recent years and it may bear potential escalating risks, especially in the case of patriotic hackers who may act autonomously with minimal to no government control. More importantly, in Southeast Asia, the absence of regional mechanisms relating to the norms and rules of State behaviour in cyberspace may bring out potential risks to the political and economic stability of the region.

The Southeast Asian cyber context tends to demonstrate a strained situation between the objective of boosting digital economies and the need to secure cyberspace. However, it can be noted that the issue of cybersecurity has been considered at regional level since the early 2000s. At the 3rd Meeting of Ministers of Telecommunications and Information Technology (TELMIN) of ASEAN in 2003, the Singapore Declaration had emphasized the need to establish the information infrastructure of ASEAN (ASEAN, 2003). The aim was to promote the interoperability, inter-connectivity, security and integrity of networks and information systems in the region. All ASEAN member states were hence to develop and implement national emergency alert and response teams (known as Computer Emergency Response Teams, CERTs) by 2005[5], in accordance with common minimum performance criteria. ASEAN's initial policy on cybersecurity has been clearly based on the idea of securing cyberspace through the development of regional cooperation in the construction of resilient national systems. National cybersecurity capacity-building continues to be emphasized as one of the main priorities in this regard, but it has been accompanied in recent years by numerous initiatives aimed at developing a regional approach to cybersecurity. For instance, the ASEAN ICT Master Plan 2015 called for the development of a common framework for network security and

[5] The process took more time than expected, the last country having set up its CERT being Laos with the establishment of LaoCERT in 2012.

the creation of the ASEAN Network Security Action Council (ANSAC) (ASEAN, 2015). The latter has convened meetings annually since 2013 and is especially responsible for reviewing the framework for cooperation on network security prepared by the ASEAN Telecommunication Regulators' Council (ATRC). The ASEAN ICT Masterplan 2020, adopted in 2016, notably comprises *"Initiative 8.1 Strengthen Information Security in ASEAN, create a trusted ASEAN digital economy', which lays the stress on data protection and critical information infrastructure; as well as 'Initiative 8.2 Strengthen Information Security Preparedness in ASEAN, improve cyber emergency responses and collaboration"*, which focuses on cyber incident emergency response cooperation. The inclusion of confidence-building measures (CBMs) appears to be a key priority of ASEAN (ARF, 2012). The ASEAN Regional Forum (ARF) is particularly active in this field. Since 2004, the ARF has organized seminars and workshops on cyberspace, with emphasis on cyber terrorism, incident response, national capacity building and the threat of proxy actors (ARF, 2012). It is worth noting that the ARF is also particularly keen on working on operationalizing cyber confidence-building measures. Moreover, the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) has integrated cybercrime among its eight priorities. Ultimately, regional cooperation regarding cyber issues is focused on reinforcement and resilience of national capacities, mobilization in the joint fight against cyber threats from criminals and terrorists together with securing the economic development of the region, and consequently, its digital economy. Capacity-building remains of utmost importance as it aims at reinforcing stakeholders' capacities at different levels to provide them with the adequate ability to respond to current and new cyber

developments and to help them govern the resources needed to deal appropriately with cyber issues[6].

Recently, several events have revealed a turning point in the region's approach to cyberspace. In May 2016, the 10th ASEAN Defence Ministers Meeting (ADMM), held in Vientiane, Laos, adopted the Philippines' proposal to establish a cybersecurity working group within the enlarged meeting of ASEAN Defence Ministers (ADMM+): the ADMM-Plus Experts' Working Group on Cyber Security. This working group could become a formal platform for the exchange of expertise and knowledge as well as the promotion of operational cooperation in the field of cybersecurity. This initiative reflects the evolution of ASEAN's approach to the issue of cybersecurity, with the inclusion of defence and military concerns in cyberspace. The ADMM-Plus EWG on Cybersecurity initiative shows that ASEAN is willing to act as a platform for confidence-building and norms development. During the ASEAN Ministerial Conference on Cybersecurity, that took place on 11 October 2016 in Singapore, Dr. Yaacob Ibrahim, the Singaporean Minister for Communications and Information and Minister-in-Charge of Cybersecurity, underlined the need to facilitate exchanges on cyber norms in Southeast Asia in his opening speech:

"[…] it is timely for ASEAN to start our dialogue on cyber norms […] Singapore notes that the 2015 report of the UNGGE made important recommendations on voluntary norms for States. Singapore is similarly supportive of having basic rules for behaviour in cyberspace. Such a set of regional cyber norms would ensure the safety and security of

[6] Capacity-building tools generally come into the form of consultative support, technical assistance and guidance, specific training sessions, sponsorship of dialogue fora etc…

regional and international cyberspace, and in extension, contribute to the stability and economic progress of the ASEAN community."

What is particularly interesting is that Dr. Yaacob Ibrahim added that: *"While staying plugged in to the global conversations, we should also make sure that norms and behaviours are kept relevant and applicable to our unique ASEAN context and cultures"* (Ibrahim, 2016). This is markedly important because it indicates that it is essential to design cyber norms that are bound to correspond to Southeast Asian nations' needs and that the region ought to play a far more proactive role in this regard. It may be noted that the ADMM-Plus is first and foremost a venue for defence and security dialogue between ASEAN member countries and the following "eight Plus countries": Australia, China, India, Japan, New Zealand, ROK, Russian Federation and the United States. As such, the ADMM-Plus EWG on Cybersecurity may benefit from potential push from some of the "eight Plus countries" to move forwards regarding cyber norms in the ASEAN region. We may wonder to what extent this new platform for regional discussion on cyber security may truly differ from other regional for a such as the ASEAN Regional Forum (ARF), which has been already pretty much involved in cyber issues.

Furthermore, during the 16th ASEAN Telecommunications and IT Ministers Meeting (16th TELMIN) on 25 and 26 November 2016, joint media statement reveals that *"[…] The Ministers were also of the view that TELMIN may serve as a platform for dedicated cybersecurity discussions in ASEAN, given the strong inter-relationships between the ICT and cybersecurity domains"* (ASEAN, 2016). On this matter, it may be noted that some ASEAN countries would be more in favour of establishing a new dedicated platform for cybersecurity[7]. It may be argued that for those who favour the

[7] Obtained through informal discussions/interviews with participants during the 16th TELMIN.

establishment of a new venue for cybersecurity, TELMIN appears to be too IT-focused, especially as cyber security requires a transverse approach. There is at least a consensus on the need to decide on appropriate ASEAN platforms for discussions on regional cybersecurity.

Working towards the definition and adoption of cyber norms in ASEAN implies to succeed in overcoming several challenges specific to the region. As mentioned earlier, the region is made up of a mosaic of countries, with diverse political regimes, disparate levels of economic development and varying degrees of cyber maturity. This regional heterogeneity creates obstacles towards regional cyber governance since it results in a differentiated approach to the challenges of securing cyberspace, primarily framed by differences in perceptions of cyberspace and its associated threats. Cyberspace has become a dimension where states reflect unique visions and strategies. In Southeast Asia, we may for instance consider the varying degree of online contents control and censorship policies, which tend to mirror the very nature of the political regimes and their position towards the flow of information. Regarding this peculiar aspect, we doubt that ASEAN would reach a common position because strict adherence to the historical principle of *non-interference* in the *internal affairs* of ASEAN member states remains the official norm, although in practice some form of flexibility does exist. The diversity of approaches to cyber issues is also a reflection of the levels of financial and human resources available to the states of the region in this field. There is also a question of differentiated political will of countries in the region: they do not necessarily have the same ambitions and do not inexorably have the same priorities in the cyber domain. Some countries may be willing to focus on certain cyber aspects (protection of critical information infrastructures, regulatory framework) whereas other countries may prefer to lay the stress on different cyber issues (promotion of local cyber security industry,

establishment of a military cyber command). The key lies in finding common priorities such as the fight against cyber-crime as exemplified by the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) which has integrated cyber-crime among its eight priorities. Further to the intrinsic diversity of the region, the development of regional cyber norms may be subject to a few internal constraints and hindrances within the ASEAN bloc.

As indicated before, the core principle of non-interference in domestic affairs may be one potential hurdle, but it seems clear that the other core principle of consensus in decision-making processes may well be the most challenging. Consensus-based decision-making requires that ASEAN members agree on a set of collective expectations regarding cyberspace and a form of common identity in the cyber domain. In this regard, there is a potential for countries to follow the norms and the rules simply for the sake of consensus. At best, this may lead to adherence to norms without a complete understanding of their value. At worst, insincere adherence to norms may occur because of the very nature of cyberspace, where attribution remains challenging. It is also important to highlight the fact that the reluctance or even mistrust of some member states towards any supranational organization, as well as the lack of coordination and compliance mechanisms for the implementation of decisions, means that most decisions taken at regional level remain dependent on their effective implementation and regulatory translation at national levels. In this regard, getting ASEAN member states to abide by the norms may well prove challenging.

Due to the ongoing trends of amplification of state-sponsored cyber espionage and militarization of cyberspace, national security issues have largely permeated cyber policy-making. Southeast Asia is no stranger to this tendency, although to date most bloc members have very recently begun to envision the strategic dimension of cyberspace.

Southeast Asia remains a region where strong nationalism prevails and ASEAN has always favoured a strong commitment to preserving and respecting national sovereignty. In this context, the elaboration of cyber norms, which would define proper state behaviour in cyberspace in conformity with a set of collective expectations, will obviously depend on the member states' true political will to engage in this work.

Cybernorms and ASEAN Realities

Heterogenous Perceptions and Valuation

Diversity in terms of disproportionate technological development in tandem with the underlying socio-political milieu compounds the challenges of norm emergence within Southeast Asia. Yet from an organizational perspective, such divisions do not appear to exist. With the establishment of the ASEAN Community, artefacts such as the ASEAN ICT Masterplan 2020 suggest a consistent conceptualization of cyberspace that serves as an enabler for socio-economic development (ASEAN, 2015). This, however, must be taken with a degree of cautious scepticism as it does not guarantee that individual members are committed to this belief.

The ideal solution to validate this alignment is to compare respective policy documents and actions against bloc pronouncements. For ASEAN, this is untenable given the lack of available sources[8]. Fortunately, this does not impede the testing of the above claim. By extending earlier threat representation research in cyberspace, state conceptualization of the domain is reflected by the corresponding threat perception (Dunn Cavelty, 2013). That is, state response to threats reflect the nature of the domain. ASEAN

[8] To date, only Singapore, Malaysia, and the Philippines have clearly identifiable national cyber strategies.

pronouncements that identify malicious code and individuals that threaten both economic and societal interests fit the discourse where the responsibility to secure is assigned to both the private sector and law enforcement bodies (ASEAN, 2011). More importantly, the referent object in this case is the business sector and individuals that depend on their services. This is aligned with existing ASEAN conceptualization of cyberspace.

This approach, however, is not without constraints. First, it cannot capture the effect that a lack of material and individual resources has on mitigating the perceived threat(s). A recurring point raised in the discourse surrounding cyber security is the costs associated with defence. This is salient given the developmental disparity amongst bloc members. Furthermore, it does not capture actors that recognize the domain's socio-economic potential while still responding to its ideational/cognitive nature. Oman, Qatar, and Turkey for instance have well developed information security capabilities yet also engage in substantial or pervasive filtering/censorship (ONI, 2017). This highlights the situation in which states continue to enforce control over cyberspace while simultaneously enjoying its economic benefits (Corrales & Westhoff, 2006).

State	ICT Development[9]	Digital Economy Dependence[10]	Information Security[11]	Silo
Singapore	HIGH	HIGH	HIGH	A
Brunei Darussalam	HIGH	HIGH	LOW	A
Malaysia	HIGH	HIGH	HIGH	A
Viet Nam	LOW	HIGH	LOW	B
Philippines	LOW	HIGH	LOW	B
Thailand	HIGH	HIGH	HIGH	A
Indonesia	LOW	HIGH	HIGH	B
Myanmar	LOW	LOW	LOW	C
Cambodia	LOW	LOW	LOW	C
Laos	LOW	LOW	LOW	C

Table 1 ASEAN Information Security Maturity

The table above appears to validate ASEAN's claim that ICT Development fosters the growth of the digital economy (ASEAN, 2011, 2015). The experience of Singapore, Malaysia, and Thailand demonstrates this causal path with high levels of ICT leading to increased importance associated with the digital economy that needs to be secured against

[9] Taken from the annual ITU ICT Development Index. The original value is converted into a two-level scale.

[10] Taken from the ASPI/ICPC Cyber Maturity in the Asia Pacific Report. The original value is converted into a two-level scale.

[11] Taken from the 2014 ITU Global Cyber Security Index (GCI). The original value is converted into a two-level scale.

potential threats. Inversely, Myanmar, Cambodia, and Laos with low levels of ICT cannot fully utilize the economic benefits of cyberspace and are thus less prone to threats to and from it due to reduce dependence. The validity of this mechanism, however, is in question with the remaining case that display high levels of dependence on the digital economy and yet exhibiting limited attempts at securing the domain (i.e. Brunei Darssalam). To elaborate this, the approach to measuring the economic dependence on the digital economy needs further discussion.

The Digital Economy Dependence indicator was obtained by asking a group consisting of government, private sector, and academia during a workshop whether (1) there is a dialogue between government and industry over cyber issues and (2) how significant is the digital economy to the national economy? This was then reflected through a 10-point scale the sum of which was used for this paper. The methodological choices of ASPI surfaces the inherent problem of measuring the actual economic impact of the digital economy and suggests that current assessments may be influenced more by perception rather than fact (Feakin, 2016). In addition, states appear to respond to high-profile events in cyberspace by securitizing the domain even in the absence of evidence demonstrating significant socio-economic or socio-political impact (Iasiello, 2013; Maness & Valeriano, 2016). Consequently, the above data appears to support the argument that attempts to secure cyberspace may be a function of decision-makers' perceptions. While this does not discount the influence of tangible realities such as technological capabilities (ICT Development), it appears to modulate rather than directly influence such decisions.

With these in mind, three distinct groups or silos are observed within ASEAN. The first, Silo A, includes states that have clearly internalized the threat to the socio-economic potential of cyberspace. Members of this group invest in not only the

technological, but the administrative and political components of information security – including the associated norms. An evaluation of the cyber strategies and policies of these states, such as Singapore and Malaysia, reflect this internalization and prioritization of the benefits offered by a secure cyberspace. The former, for instance, acknowledges that disruptions caused by malicious actors have a direct and debilitating effect on economies (CSA, 2016). Similarly, the Malaysian National Cybersecurity Policy notes that a secure infrastructure will *"promote stability, social well-being and wealth creation"*. This reflects an alignment with a conceptualization of cyberspace contained in the ASEAN roadmaps (MOSTI, 2013). Empirically, these states also invest significantly larger portions of their GDP into cybersecurity compared to others within the region – with Singapore far exceeding the global average (0.22% of GDP) (ATKearney, 2018).

The second, Silo B, are those that recognize the presence of such threats, but may prioritize other issues resulting in limited resources being dedicated towards cybersecurity resulting in partial attempts to secure the domain. Viet Nam's 2015 Cyber Information Security Law typifies this dilemma. While the law clearly acknowledges the state's susceptibility towards malicious behaviour and its implications, it appears torn between protecting infrastructure and enforcing content control over their citizen's activities in cyberspace (Gray, 2016). Furthermore, states in this silo invest significantly less in cybersecurity compared to the global average (0.03% of GDP vs 0.13%) (ATKearney, 2018). These suggest that while a superficial similarity with Silo A exists in terms of how cyberspace is perceived, the observed actions suggests otherwise.

Finally, Silo C is composed of those that do not recognize the threat due to the absence of assets that are placed in harm's way. This would be typical of states that have yet to benefit from the digital economy. Using Internet access as a point of comparison, an average of 70.83% of Silo A's population have access to the Internet. In contrast, only

24.17% of Silo C's enjoy the socio-economic benefits of Internet access[12]. Consequently, political will to secure this domain is unsurprisingly absent given the limited consequences that may emerge from the exploitation of cyberspace by malicious actors.

While this analysis is regionalized to ASEAN, a similar process may be observed in other states as well. Using existing models, states that enjoy greater socio-political cohesion have called for and accepted norms aimed at ensuring the stability of cyberspace and its infrastructure. States such as the United States, the United Kingdom, and Germany are representative of this. In contrast, states such as Russia and China where stability is a function of accepting the existing regime's narrative has called for norms regulating the free flow of information that may challenge these said narratives.

Although this paper argues from the perspective of economic policy, the underlying logic remains the same. Because these different silos benefit (or not) from cyberspace in differing ways, their view of the domain and the norms associated vary consequently. Given these differences, one can deduce a divergence across these three silos of their respective conceptualization of cyberspace. Since the promotion of norms is predicated on shared beliefs, these signal significant challenges to the acceptance of cyber norms within the region. These, however, are not insurmountable.

Scholars have argued for a pluralistic format where like-minded states could easily come together to form norms that match their existing beliefs (Grigsby, 2017; Lewis, 2011). In this manner, obstacles resulting from varying conceptualizations of cyberspace do not serve as a hindrance for the emergence and acceptance of cyber norms. Within ASEAN, individual silos may adopt this format to begin the process of norm building. This, however, only forms the initial steps to bridge the gap between these

[12] Silo B average 42.46% respectively.

groups that may lead to region-wide cyber norms. To overcome this, two complementary steps are required.

While member states continue to experience disparities in terms of infrastructure and capabilities, cooperation may be achieved through confidence-building measures (CBM). Unlike norms that require shared principles and beliefs, CBMs can flourish because of a common (and practical) interest in preventing conflict and/or escalation amongst states. This serves as the initial step towards the establishment of region-wide norms. CBMs such as information and expertise exchange in the form of cooperation between Computer Emergency Response Teams (CERTs) would benefit states that exist in different silos. For example, Viet Nam has been identified as a notable source of malware within the region that may threaten infrastructure (and individuals) in other states such as Singapore. As such, it would be beneficial for both to exchange knowledge and expertise in mitigating these threats such that the later would improve its cybersecurity standing globally while the former can ensure the continued security of its infrastructure. Although these and similar initiatives would not remove the barriers that result in the emergence of these silos, these increase the level of trust between member states.

Besides building trust, ASEAN could also engage in capacity-building measures aimed at assisting less develop members in enhancing their respective cyber infrastructures. This is not a novel idea as it has been acknowledged in both the past and current ASEAN Master Plans. However, this paper argues that doing so not only serves to meet the socio-economic objectives of ASEAN but also encourages the development of shared beliefs in cyberspace which, for the region, is grounded in the economic benefits of the domain.

While a shared conceptualization of cyberspace remains absent amongst bloc members, the failure of norms is not a forgone conclusion. Confidence-building measures between silos and capacity-building measures aimed to assist socio-economic development serve as practical solutions in efforts to establish region-wide cyber norms. Furthermore, processes such as the ASEAN Minus X mechanism are in place that can assist in these endeavours.

ASEAN Bridging Mechanisms

The above proposal towards the establishment of regional cyber norms must be put in perspective not only with the ASEAN Way but more importantly with the ASEAN Minus X mechanism. The ASEAN Way refers mostly to the fact that consensus is the privileged mode of decision-making in ASEAN and that minimal institutionalization and collective consultation remain key in respect to any implementation of a regional initiative or project. As for the ASEAN Minus X mechanism, it was introduced in the 1980's and allows for willing member states to move forwards in specific areas whereas others would participate when ready (ASEAN, 2007)**.** This process allows for flexible participation in cases where a member state is not yet ready to commit to a specific initiative or project. Given the supremacy of consensus within ASEAN, this mechanism enables the organization to overcome potential deadlocks on the road to progress in regionalization. As such, the ASEAN Minus X mechanism is particularly relevant when the member states fail to reach full consensus. However, it should be highlighted that this mechanism had been primarily designed along economic lines, i.e., in the case of initiatives and projects relating to economic cooperation. The philosophy of the ASEAN Minus X mechanism has already been applied several times and firstly during the construction process itself of ASEAN where Philippines, Indonesia, Malaysia, Singapore, and Thailand stood as founding countries, followed by Brunei who joined them six days after independence

from the United Kingdom on 8 January 1984. Vietnam entered in 1995, followed by Laos and Burma (now Myanmar) on 23 July 1997 and Cambodia on 30 April 1999. There are other examples such as the adoption of the ASEAN Convention on Counter-Terrorism (ACCT) which was signed in 2007. *"As stipulated in the ACCT, the Convention enters into force 30 days after the sixth ASEAN Member State submits its instrument of ratification with the Secretary-General of ASEAN. Brunei Darussalam became the sixth country to ratify it on 28 April 2011 and the ACCT came into force on 27 May 2011"* (ASEAN, 2013). It is no earlier than 2013 that the last member of the ASEAN ratified the ACCT but the Convention had been already in force since 2011. So far, there have been discussions within ASEAN about the opportunity to extend this mechanism to other domains, especially regarding political and security issues as well as social and cultural issues but it seems that the organization has not reached a common position on the subject.

Given the current mechanisms in place within ASEAN, it would be interesting to see whether member states would be willing to and could come out with an extension of the ASEAN Minus X mechanism with regards to the implementation of a siloed approach to cyber norms design for the region. As there is little chance that full consensus would be reached in this area, due to the various reasons exposed in previous sections, this unique mechanism of ASEAN would enable member states, who are willing to commit, to engage in the process of working towards cyber norms in the region while allowing for other member states to join later when better prepared and readied.

Regarding salient security issues in the region, we may note that several non-military security cooperation frameworks have been established by ASEAN, such as the Zone of Peace, Freedom and Neutrality (ZOPFAN) declaration in 1971, the Treaty of Amity and Cooperation (TAC) in 1976, the ASEAN Regional Forum (ARF) in 1994 and the Southeast Asian Nuclear-Weapon-Free Zone Treaty (SEANWFZ), also known as the

Treaty of Bangkok, in 1995. These initiatives were all based on the main thrusts of conflict prevention and peaceful conflict resolution. As both the internal and external strategic environments of ASEAN had evolved since the 1990s, there was a need to think about norms and processes regarding renewed intra-regional disputes as well as new transnational threats together with the strategic return of the U.S., the evolving developments in Northeast Asia and the terrorist attacks on the United States of September 2001. At the turn of the 2000s, the idea of an ASEAN Security Community, as described in the Declaration of ASEAN Concord II (Bali Concord II) of 2003 and put forward by Indonesia, reflected the broader objective of establishing modalities for norms-setting, conflict prevention, conflict resolution and post-conflict peace-building in Southeast Asia. Since then, ongoing discussions between ASEAN member states paved the way for the formulation of the ASEAN Political-Security Community, Blueprint 2025, which was released in March 2016 (ASEAN, 2016). It is worth mentioning that the main components of the blueprint had been discussed and validated in 2013, during the 23rd ASEAN Summit in October 2013. As far as cyber issues are concerned, section B.3.6. ‘Strengthen cooperation in combating cybercrimes’ is the only part of the document devoted to tackling cybersecurity, and what is more in a very narrow scope, where solely cybercrime and cyber-terrorism appear to be the two major concerns. Moreover, this section sticks to very general issues such as information sharing, law enforcement and awareness. As a matter of fact, regional cooperation against cyber criminality strictly speaking has already been a work in progress for some time and as such the ASEAN Political-Security Community, Blueprint 2025 brings out nothing new in this regard. As mentioned before, the most interesting recent regional developments regarding the cyber domain are the ADMM-Plus EWG on Cybersecurity initiative and Singapore support for having basic rules for behaviour in cyberspace in the region.

As the quest for peace and security in the region lies at the heart of the birth and development of ASEAN, and as the organization has already shown that it had been able to work out several regional security cooperation frameworks, we may wonder whether working together on regional cyber norms would enable member States to advance regional progress on the road to the enhancement of the ASEAN Political-Security Community pillar as part of the broader agenda of the ASEAN Community objective. In the context of our proposal for a siloed approach toward working cyber norms in ASEAN, we may remind the implementation process of the Southeast Asia Nuclear Weapon Free Zone Treaty (SEANWFZ). Although it falls into the specific category of a treaty and more specifically regarding nuclear weapons, which we cannot transpose into the cyber domain, a few process and implementation features shall be highlighted. Firstly, some member States appeared to have been the key advocates of the treaty, i.e. Indonesia and Malaysia. Both countries started as early as the 1970s to push the idea forward. This means that new initiatives within the organization have best chances to come out when sponsored or at least supported initially by a few member States. Secondly, at the beginning of the discussions process, the U.S. expressed strong opposition to the idea of the treaty and consequently Thailand, the Philippines and Singapore appeared to be reluctant to go forward. The lesson here to be learned is that, as ASEAN is part to multilateral organizations, especially the ARF and the Asia-Pacific Economic Cooperation (APEC), and due to the transnational and trans-regional nature of the cyber domain, external parties may be willing to have their say. This may not as such hinder the regional process but ASEAN would have to consider extra-regional initiatives regarding cyber norms.

Conclusion: Moving Forward

The previous sections have highlighted the unique challenges and opportunities facing

ASEAN in its efforts to promote cyber norms. Unbalanced utilization of cyberspace in conjunction with heterogenous threat perceptions are expected to result in the emergence of incongruent norms amongst members of the bloc. Although unfavourable, ASEAN mechanisms do allow for members with disparate views to enter into agreement later. Consequently, the greater challenge is not the initial emergence of incongruent norms, but rather, how to bridge these differences.

The decision to invest in cyberspace as an enabler of socio-economic progress is manifested in the existing ASEAN ICT Masterplans and corresponding projects. As noted in its completion report, its stated objectives of Economic Transformation, People Engagement and Empowerment, Innovation, Infrastructure Development, Human Capital Development, and Bridging the Digital Divide have been met with great success over the period of 2011 to 2015. Moreover, a review of key indicators supports its claim that ICT, and in turn cyberspace, has further established itself within the bloc with respect to infrastructure and use. These developments, however, must be taken with a grain of salt. Although these technologies are proving to be increasingly accessible compared to a decade ago, increased access does not immediately lead to usage and dependence. Concepts that have been identified as crucial in the valuation of this domain and corresponding threat perceptions.

The completion report highlights trust issues that still exist and limit the degree in which these technologies are employed within a given society. While the barriers of entry may have indeed been lowered, the extensive use of cyberspace for crucial socio-economic transactions remains absent. Related studies such as the Asia-Pacific Cyber Maturity Index note that the absence of appropriate legislature that regulates behaviour and ensures safety is a barrier for deeper adoption of this man-made domain. Specifically, it notes that this is particularly relevant in the case of the CLMV where efforts have

focused on infrastructure development at the cost of these supporting instruments. Citing the findings presented in the earlier section, these same countries are also the least likely to view cyberspace as an enabler for economic development.

Moving forward, ASEAN should take this into account as it begins to roll out its 2020 ICT Masterplan. Unless trust in the cyberspace is strengthened through cybersecurity measures, its socio-economic value in societies across the region will continue to remain inconsistent and superficial. This limits the perceived value of the domain that, in turn, tempers the sense of urgency needed to protect it from potential threats. This process is crucial for the emergence of cyber norms.

To overcome these issues, the paper suggests a dual process of confidence and capability building measures. The former aims to improve cooperation between different members that may not share a common understanding of cyberspace. Activities such as the annual ASEAN Computer Emergency Response Team Incident Drill (ACID) aims to enhance indecent response within the region thus increasing trust in the stability of the domain. Furthermore, it also fosters greater cooperation between bloc members. The later, in contrast, is meant to enhance the capabilities of individual states and has been a corner stone of the ASEAN Master Plan since its inception. In doing so, this allows less developed states to enjoy the socio-economic benefits of cyberspace thus encouraging greater parity in terms of the conceptualization of cyberspace within the region.

The solution proposed thus far does not guarantee that cyber norms will take root within the region. By acknowledging the obstacles that face this initiative, however, the paper offers a possible solution that increases the chances of success for ASEAN. Furthermore, these lessons need not be limited to the experience of Southeast Asian states. While the prevailing conditions are indeed different in other region, variations in the conceptualization of cyberspace and its associated threats continues to be an enduring

problem that has plagued efforts to established norms within cyberspace. Consequently, in recognizing these constraints, both scholars and policy makers are in a better position to provide solutions that further guarantees stability in this increasingly relevant domain.

Bibliography

ARF. (2012). *Co-Chairs' Summary Report of the ARF Seminar on Confidence Building Measures in Cyberspace*. Retrieved from http://www.mofa.go.jp/files/000016406.pdf

ASEAN. (2003). *Joint Media Statement of the 3rd ASEAN Telecommunications and Information Technology Ministers Meeting, Singapore*. Retrieved from http://asean.org/joint-media-statement-of-the-3rd-asean-telecommunications-and-information-technology-ministers-meeting-singapore-19-september-2003/

ASEAN. (2007). *Charter of the Association of Southeast Asian Nations*. Retrieved from http://www.asean.org/wp-content/uploads/images/archive/21069.pdf

ASEAN. (2011). *ASEAN ICT Masterplan 2015 Completion Report*. http://www.asean.org/storage/images/2015/December/telmin/ASEAN%20ICT%20Completion%20Report.pdf.

ASEAN. (2013). *ASEAN Convention on Counter-Terrorism Completes Ratification Process*. Retrieved from http://asean.org/asean-convention-on-counter-terrorism-completes-ratification-process/

ASEAN. (2015). *ASEAN ICT Masterplan 2020*. Retrieved from https://www.trc.gov.kh/wp-content/uploads/2016/10/1.pdf

ASEAN. (2016). *16th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings, Bandar Seri Begawan, Brunei Darussalam, 26 November 2016, Joint Media Statement*. Retrieved from http://asean.org/storage/2012/05/TELMIN-16-JMS-Final-cleared.pdf

ASEAN. (2017). *Chairman's Statement of the 2nd ASEAN Ministerial Conference on Cybersecurity*. Retrieved from http://asean.org/storage/2012/05/2nd-AMCC-Chairmans-Statement-cleared.pdf

ATKearney. (2018). *Cybersecurity in ASEAN: An Urgent Call to Action*. ATKearneyhttp://www.southeast-asia.atkearney.com/documents/766402/15958324/Cybersecurity+in+ASEAN%E2%80%94An+Urgent+Call+to+Action.pdf/ffd3e1ef-d44a-ac3a-9729-22afbec39364.

Betz, D. J., & Stevens, T. (2011). Power and Cyberspace. *Adelphi Series, 51*(424), 35-54

CCDCOE. (2017). *Cyber Definitions*. Retrieved from https://ccdcoe.org/cyber-definitions.html

Corrales, J., & Westhoff, F. (2006). Information technology adoption and political regimes. *International Studies Quarterly, 50*(4), 911-933

CSA. (2016). *Singapore Cybersecurity Strategy*. Singapore: Cybersecurity Agency of Singapore Retrieved from https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf.

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review, 15*(1), 105-122

Feakin, T. W., J.; Nevill, L. & Hawkins, Z. (2016). *Cyber Maturity in the Asia-Pacific Region*. Canberra, Australia.

Finnemore, M. H., Duncan B. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law, 110*(3), 425-479. doi: 10.5305/amerjintelaw.110.3.0425

Forsyth Jr, J. W., & Pope, M. B. E. (2014). Structural Causes and Cyber Effects Why International Order is Inevitable in Cyberspace. *Strategic Studies Quarterly, 8*(4)

Gray, M. L. (2016, 21.10.2016). *The Trouble with Vietnam's Cyber Security Law*. Retrieved from https://thediplomat.com/2016/10/the-trouble-with-vietnams-cyber-security-law/
Grigsby, A. (2017). The End of Cyber Norms. *Survival, 59*(6), 109-122
Hare, F. (2010). The Cyber Threat to National Security: Why Can't We Agree? *Conference on Cyber Conflict, Proceedings 2010*, 211-225
Iasiello, E. (2013). Cyber attack: A dull tool to shape foreign policy *Cyber Conflict (CyCon), 2013 5th International Conference on* (pp. 1-18): IEEE.
Ibrahim, Y. (2016, 10.11.2016). *Opening Speech by Dr Yaacob Ibrahim, Minister For Communications And Information And Minister-In-Charge Of Cybersecurity, At The Asean Ministerial Conference On Cybersecurity*. Retrieved from https://www.csa.gov.sg/news/speeches/minister-yaacob-speech-for-amcc-2016
Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. S. Kramer, Stuart H.; Wentz, Larry (Ed.), *Cyberpower and National Security* (pp. 24-42). Dulles: Potomac Books.
Lewis, J. A. (2011). Confidence-building and international agreement in cybersecurity *Disarmament Forum* (Vol. 4, pp. 51-59).
Lindsay, J. R. (2014). The Impact of China on Cybersecurity Fiction and Friction. *International Security, 39*(3), 7-+
Luiijf, H. A. M., Besseling, K., Spoelstra, M., & De Graaf, P. (2011). Ten national cyber security strategies: A comparison *International Workshop on Critical Information Infrastructures Security* (pp. 1-17): Springer.
Maness, R. C., & Valeriano, B. (2016). The Impact of Cyber Conflict on International Interactions. *Armed Forces & Society, 42*(2), 301-323. doi: 10.1177/0095327x15572997
Markit, I. (2017). *IHS Jane's Defence Budgets Annual Reports*. https://www.ihs.com/products/janes-defence-budgets.html.
Mazanec, B. M. (2015). Why International Order in Cyberspace Is Not Inevitable. *Strategic Studies Quarterly, 9*(2)
MOSTI. (2013). *The National Cyber Security Policy*. Ministry of Science, Technology and Innovation Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Malaysia%20Cyber%20Security%20Policy.pdf.
Nye, J. S. (2014). *The Regime Complex for Managing Global Cyber Activities*. C. House.
Obama, B. (2015). *Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference*. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint
ONI. (2017). *Country Profiles*. Retrieved from https://opennet.net/country-profiles
Rivera, J. (2015). Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk. *2015 7th International Conference on Cyber Conflict - Architectures in Cyberspace (Cycon)*, 7-24
Rõigas, H. (2015, 10.02.2015). *An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?* Retrieved from https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html
Tran Dai, C. S., K.; Douzet, F.; Nocetti, J.; Desforges, A.; Robine, J.; Samaan JL (2014). *Géopolitique du cyber en Asie*. Paris.
UN-GGE. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

UN. (2011). *International code of conduct for information security*. Retrieved from https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf

Väljataga, A. (2017). *Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly*. Retrieved from https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html