"NORM SUBSIDIARITY" OR "*NORM DIFFUSION*"? A CROSS-REGIONAL EXAMINATION OF NORMS IN ASEAN-GCC CYBERSECURITY GOVERNANCE

Hanan Mohamed Ali, School for International Studies, Simon Fraser University

Abstract

Cybercrime has been a contentious issue among security actors, vis-à-vis the extent to which international cooperation may be fostered to respond to the accelerating incidence of cyber-attacks. This paper contrasts between the cyber-governance approaches adopted by two non-Western regional organizations, the Association of Southeast Asian Nations and the Gulf Cooperation Council, over the past decade. Considering their similar institutional origins, Most Similar Systems Design methodology was employed to assess how ASEAN and GCC have *distinctly* responded to cybercrime. It considers the dynamics of the digital divide — a divide which is exacerbated by the COVID-19 pandemic — and in which ASEAN and the GCC are challenged to bolster their cyber-capabilities. Findings reveal that GCC increasingly *diffuses* norms of international cooperation to tackle cybercrime. By contrast, ASEAN embodies cyber norms which regulate behavior along the lines of intra-regional cooperation, wherein norms of international cooperation are rendered *subsidiary* to norms of regional autonomy.

Introduction

On October 2010, the Ministry of Post and Telecommunications in Myanmar — a member-state of the Association of Southeast Asian Nations (ASEAN) —was subject to a series of Distributed Denial of Service (DDoS) attacks, right before the country's first national election in twenty years, in an attempt to restrict the flow of information over the election period (Broeders & van den Berg, 2020).

Two years later, in 2012, an organization at the University of Toronto — Citizen Lab — located the use of a digital surveillance tool named "Finfisher" in Bahrain, Oman, Qatar, Saudi Arabia, Kuwait, and the UAE, all of which form the Gulf Cooperation Council (GCC). Described by Citizen Lab as malware, Finfisher had been used to obtain information from the devices of pro-democracy activists in the Gulf states, where there had been extensive protests against government during the Arab Spring of 2011 (Shires & Hakmeh, 2020).

The accelerating frequency of cyber-attacks in the Persian Gulf and Southeast Asia has been a point of contention among regional security analysts, vis-à-vis the extent to which international cooperation constitutes the best solution by

which to tackle cybercrimes. These concerns, thus, inform the research question: How have the GCC and ASEAN *distinctly* responded to the accelerating incidence of cybercrime within their respective regions? To answer this question, this paper will argue: While GCC member-states have focused their efforts on establishing mechanisms for international cooperation to tackle cybercrime threats (via "norm diffusion"), most ASEAN member-states are oriented towards the legitimization of national and regional cooperation in cyberspace (via "norm subsidiarity").

The importance of this thesis lies in the *variant* approaches taken by the GCC and ASEAN, despite sharing similar institutional traits and experiencing similar cyber-vulnerabilities. A Most Similar Systems Design (MSSD) methodology will be employed to support the following causal mechanism which forms the core of the thesis: Uneven cyber-capabilities — among ASEAN member-states *as well as* between ASEAN and the GCC — impacts perceptions as to what constitutes the optimal solution to tackle cybercrime and, correspondingly, the level (national, regional, or international) at which cooperation should be concentrated. The independent variable in this causal mechanism is even/uneven levels of cyber-capability, whereas the dependent variable is the distinct cooperation approaches taken (national/regional versus international) which are specifically embodied in either *subsidiary* cyber-norms or the *diffusion* of global cyber-norms. Thus, the mechanism tying the link between the level of cyber-capabilities (IV) and the nature of cooperation approach to tackle cybercrime (DV) is the role of norms (*subsidiary* norms or *diffuse* norms).

To further unpack the thesis, it is critical to provide some conceptual clarity. Firstly, international cooperation is conceptualized by the extent to which security actors have or have not made efforts to participate in the exchange of information (i.e., threat intelligence), expertise, assets (i.e., facilities, equipment, technology), and other resources within officially recognized multilateral agreements. It is also characterized by the participation of security actors in international fora, cyber-drills, conferences and training (e.g., The World Summit on Information Society, the Global Forum on Cyber Expertise, and the Internet Governance Forum). The greater the levels of international cooperation, the stronger one's cybersecurity capabilities to deter cybercrime attacks and enable better investigation, apprehension, and prosecution of malicious agents. Given the transnational, complex, and unpredictable nature of cybercrimes, the need to foster international cooperation cannot be overstated.

Secondly, cybersecurity is defined as "transnational or cross-border interaction and effect in and across the levels of cyber activities that are considered to impact international peace and security" (Tikk & Kerttunen, 2020, p. 37). Thirdly,

"cybercrime" refers to a category of malicious online activity which involves both private- or state-controlled cyber attackers targeting foreign governments and high-value businesses in order to steal sensitive information for commercial, military, and political gain (Shackelford & Craig, 2014, p. 5). Finally, "norms" refer to shared expectations of "responsible state behavior" in cyberspace (Tikk & Kerttunen, 2020, p. 55).

To provide a roadmap, the paper will entail a Literature Review section discussing scholarly debates on cyber-sovereignty and multistakeholder governance approaches to tackle cybercrime. It will also address lacunae in understandings of cyber-governance by adapting Amitav Acharya's analytical framework of "norm subsidiarity" and "norm diffusion". Followed by this is a Methods section justifying case and MSSD selection, as well as a section on the Regional Hurdles faced by both regional organizations in tackling cybercrime: i) the digital divide; ii) lack of harmonization. Then, two separate sections on the Analysis of GCC-ASEAN Responses to Cybercrime will empirically focus on the dynamics of "norm subsidiarity" and "norm diffusion", in relation to the regional hurdles identified prior. Finally, the Conclusion will reinforce the paper's substantive findings and consider how those findings may provide pathways for future research.

Literature Review

The existing literature has produced meaningful insights about cybersecurity governance models adopted by security actors to address a myriad of cyber threats ranging from cyber-terrorism, cyberwarfare, and cyberespionage to cybercrime. Cybersecurity governance is dichotomized between "cyber-sovereignty" and "multistakeholderism".

Emerging from the early 1990s, cyber-sovereignty emphasizes state control over internal information and communications technology (ICT) infrastructures (Perritt, 1997; Trachtman, 1998). The latter promotes participation between governments, civil society, and high-value organizations to combat cyber-threats. Scholars of cyber-sovereignty, such as Bartelson et al. (2018), claim that cyberspace requires a governance approach based on ideas of state sovereignty and territoriality — akin to a "cyber Westphalia" (p. 35). To have strictly demarcated sovereign authorities governing an otherwise abstract domain, Barcomb et al. (2012) argue that every piece of ICT infrastructure is tied to a "specific geographic location and is owned, operated, and maintained by some entity" (p. 493). Given that cybercrime is seen as a threat to national security, sovereignty claims provide the basis for strengthening national security objectives in cyberspace, and shields countries from external cyber-aggression.

As a counterpoint to cyber-sovereignty, liberal multistakeholder views grew popular in the early 2000s. Scholars of multistakeholderism contest the applicability of sovereignty to cyberspace in favor of multistakeholder internet governance (MSG). Notable proponents of MSG, Hemmati et al. (2002) and Hoffman (2016), claim that the best mechanism for maintaining open and cooperative policy dialogue-informed by a broad range of stakeholders—including businesses, technical experts, governments, and civil society—is reaching consensus through a bottom-up approach. This governance approach insists upon a) effectiveness (in maximizing favorable results while minimizing unfavorable outcomes) and b) alignment with stakeholder values (which essentially means embodying those values and norms that are increasingly commonplace, including participation, reciprocity, and freedom of expression) (Hemmati, 2002, p. 11).

While there exists a substantive body of research concerning cybersecurity governance to tackle cybercrime, gaping holes in the literature remain. The literature paints a clear picture of cybersecurity governance, though it is an oversimplified one that fails to encapsulate the domain's complexities specific to the regions under study. The cybersovereignty-multistakeholder dichotomy, for instance, is emblematic of the ethnocentric bias (and resultant false universalisms) in International Relations (IR) theory. That is, the bias towards theorizing about global cyber-governance by over-privileging Western principles, ideas, and practices, while non-Western experiences remain under-theorized. This has led to tendencies to view Western cyber-governance models as the universal standard by which all security actors ought to emulate; meanwhile, non-Western practices that stray from this standard are observed as mere particularisms. In this case, such false universalism is aptly illustrated by the disconnect between the elements of IR theory derived from Western experience — i.e., the dichotomization of cybersecurity governance between cyber-sovereignty and multistakeholderism — versus the practices actually employed by non-Western regional institutions.

To paint a more composite picture, therefore, this paper focuses on the role of norms by regionalizing and adapting Acharya's theory of "norm subsidiarity" and "norm diffusion" to ASEAN and the GCC. He defines "norm subsidiarity" as "a process whereby national [or regional] actors create rules with a view to preserve their autonomy from dominance, neglect, violation, or abuse by more powerful central actors" (Acharya, 2011, p. 97). The concept originates from the general meaning of subsidiarity which refers to "a principle of locating governance at the lowest possible level — that closest to the groups affected by the rules and decisions adopted and enforced" (Slaughter, 2004, as cited in

Acharya, 2011, p. 97). In "subsidiarity," local/regional security actors reject external ideas of "powerful central actors," namely due to great-power violations of global norms and the unwillingness or inability of high-level institutions to prevent those violations — as evidenced by the great-power competition and interventionism of the Cold War, as well as the subsequent paralysis of the UN. On the other hand, "norm diffusion" is the process wherein global norms are "socialized and shared, and then become internalized, accepted, and implemented" (Acharya, 2011, p. 97) by national or regional actors (Taddeo, 2018).

The analytical relevance of Acharya's (2011) theory to a cross-regional study of ASEAN-GCC cyber-governance lies in its specific ability to explain how non-Western states and regions engage in their own forms of norm-creation, thereby moving beyond a conception of rule-making as a fundamentally Western enterprise. In this paper, therefore, Acharya's (2011) theoretical framework is used to suggest that uneven cyber-capabilities (IV) have produced *distinct* cooperation approaches among the GCC and ASEAN, neither of which fit within the binary model theorized by Bartelson et al. (2018), Barcomb et al. (2012), Hemmati et al. (2002), and Hoffman (2016).

The GCC's cooperation approach occupies a hybrid position between both camps since it diffuses cyber-sovereign norms *and* multistakeholder norms as a strategic mechanism for facilitating *international* cooperation. *Contrastingly*, ASEAN's responses to cybercrime have centered around *national/regional* cooperation, though it does not embody cyber-sovereign norms. The ASEAN Regional Forum has shown support for multistakeholder norms, specifically the norms laid out by the UN Group of Governmental Exerts in 2015, though it does not embody them. Rather, cyber-sovereign and multistakeholder norms are rendered *subsidiary* to norms of regional autonomy at the heart of the organization. Thus, ASEAN occupies a position wherein it is neither a proponent of cyber-sovereignty nor of multistakeholderism.

Methods

Regarding methods, ASEAN and the GCC will be analyzed through Most Similar Systems Design (MSSD). In comparative research, MSSD is based on selecting cases that share many important characteristics, but differ in one crucial aspect (Halperin & Heath, 2020). The common characteristics act as a *control* to test whether the crucial difference between the cases is associated with the variation in the dependent variable (distinct cooperation approaches to cybercrime, in this case) (Halperin & Heath, 2020).

ASEAN and the GCC were selected as they are *similar* in virtue of their institutional origins, traits, security orientations, and vulnerabilities to cybercrime attacks (considering the strategic value of both regions).

For example, both share similar institutional beginnings. The political role of ASEAN and the GCC as a forum for preventing, managing, and resolving conflicts among their members was a major part of the rationale behind their creation (Job, 1992). The creation of ASEAN in 1967 reflected a strong desire on the part of the original five members — Malaysia, Indonesia, Singapore, Thailand, and the Philippines — to minimize prospects for intra-regional conflict (Job, 1992). This political role of ASEAN was institutionalized thereafter via the creation of a mechanism for conflict resolution at the Bali summit in 1976, under articles 13-17 of the Treaty of Amity and Cooperation (Job, 1992). Similar to ASEAN, the role of the GCC (established in 1981) in dispute resolution among its members is articulated in its charter. Therefore, the ultimate goal for both organizations is to create a "security community" in which their members develop "dependable expectations of 'peaceful change'" in intraregional relations (Job, 1992, p. 51). The security orientation of both ASEAN and the GCC also rests upon preserving regional autonomy against foreign intervention. Dating back to the time of their inception, member-states of both organizations were proponents of regional autonomy, with ASEAN launching the Zone of Peace, Freedom and Neutrality (ZOPFAN) framework and the GCC calling for the "Gulfanization of Gulf security" (Amirahmadi & Entessar, 2002, p. 149).

Additionally, both organizations have to grapple with increasing cyber-vulnerabilities and attacks. Networks within the ASEAN Secretariat, as well as among its member-states, have been undermined by Advanced Persistent Threat (APT) attacks (Eggenschwiler, 2018). APT attacks are defined as cybercrime attacks which target specific entities to steal their data via computer hacking processes; these attacks are designed to steal trade secrets, intellectual property, and other confidential information from governments and leading companies in the Asia-Pacific region (Eggenschwiler, 2018). For example, extensive APT attacks were launched during the 2016 South China Sea dispute in which China, Vietnam, and the Philippines had competing territorial claims (Tikk & Kerttunen, 2020). Malware — such as "Gamarue" and "PLATINUM" — were detected by Microsoft in 2016 as these computer worms enabled hackers to control infected systems and procure information related to the dispute (Tikk & Kerttunen, 2020). The Philippines Department of Justice (DOJ), representatives of the Asia-Pacific Economic Cooperation (APEC) summit, and an international law firm were also targeted in an APT cyber-attack over their involvement in the disputed South China Sea (Tikk & Kerttunen, 2020). A malicious program —"NanHaiShu" —

was identified as the APT deployed to install Remote Access Trojans (RAT) into target systems through spear-phishing emails and electronic communications scams (Tikk & Kerttunen, 2020).

Similar to ASEAN, the landscape of cybercrime in the GCC stretches from DDoS attacks on key government departments and APT attacks to malware threats targeted at the energy sector, online influence operations, as well as hack-and-leak intrusions. Such attacks on GCC's information systems have been the focus of cybersecurity efforts since the 2011 Arab Spring, which represented a new wave of dangers against digital communications technologies (Shires, 2019). Cybercrime threats have also attracted renewed attention due to internal divisions within the GCC following the Qatar embargo in 2017 (Shires, 2019).

Not to mention, both regional organizations are geographically more compact, culturally less heterogeneous, and consist more of politically like-minded member-states in comparison to the membership of larger regional groups such as the Organization of African Unity or the League of Arab States (Job, 1992).

Despite the similarities, they have various independent variables which need to be isolated, one of which will subsequently justify the different outcome (variegated cooperation approaches to tackle cybercrime) across these two cases. To support the argument, an MSSD research design will demonstrate that the evenness of cyber-capabilities is the independent variable that can account for differences in cybersecurity cooperation approaches — the dependent variable (See Tables 1 & 2).

Tables 1 & 2 show that the top countries with the greatest cyber-capabilities (measured by cybersecurity preparedness and ICT development) were Saudi Arabia, Oman, Qatar, the UAE, Singapore, and Malaysia, while countries with the least cyber-capabilities were Laos, Myanmar, Cambodia, Vietnam, and the Philippines. Since different states have varying conceptualizations of cybercrime threats (the immediacy of those threats), Tran Dai and Gomez (2018) have developed a typology by which it is possible to capture three common conceptualizations and to categorize states into three silos (A, B, C), accordingly.

This paper borrows Tran Dai and Gomez's (2018) typology in line with ASEAN and the GCC's ICT development levels and cybersecurity preparedness scores to provide a comprehensive operational measure of cyber-capability (the IV), as shown in Tables 1 & 2. Based on whether member-states from both organizations I) recognize the issue of cybercrime and developed its ICT infrastructures accordingly; II) recognize the presence of cybercrime threats, but may have various competing priorities that inhibit the development of ICT infrastructures;

or III) fail to recognize the magnitude of cybercrime. They are then categorized under distinct silos: Silo A, Silo B, or Silo C (Tran Dai & Gomez, 2018). It is noteworthy that most ASEAN members are either categorized under Silo B or Silo C, with the exception of Singapore and Malaysia (Silo A), reflecting *uneven* levels of cyber-capability in the region. The fact that most of the GCC member-states are categorized under Silo A, with the exception of Kuwait and Bahrain (Silo B), is attributable to the relative *evenness* of cyber-capability in the region.

Table 1: Measuring The Independent Variable (Level of Cyber-Capabilities) in ASEAN

ASEAN Member-States	ICT Development	Cybersecurity Preparedness Score	Silo
Singapore	**HIGH**	**0.898**	**A**
Malaysia	**HIGH**	**0.893**	**A**
Brunei	**LOW**	**0.624**	**B**
Vietnam	**LOW**	**0.693**	**B**
Philippines	**LOW**	**0.543**	**C**
Thailand	**HIGH**	**0.796**	**B**
Indonesia	**LOW**	**0.776**	**B**
Myanmar	**LOW**	**0.172**	**C**
Cambodia	**LOW**	**0.161**	**C**
Laos	**LOW**	**0.195**	**C**

Source: *International Communications Union Global Cybersecurity Index (2018)*

Table 2: Measuring The Independent Variable (Level of Cyber-Capabilities) in GCC

GCC Member-States	ICT Development	Cybersecurity Preparedness Score	Silo
Saudi Arabia	**HIGH**	**0.881**	**A**
Oman	**HIGH**	**0.868**	**A**
Qatar	**LOW**	**0.860**	**A**
United Arab Emirates	**LOW**	**0.807**	**A**
Kuwait	**LOW**	**0.600**	**B**
Bahrain	**HIGH**	**0.585**	**B**

Source: *International Communications Union Global Cybersecurity Index (2018)*

Analysis

ASEAN's Regional Hurdles

Despite ASEAN's pledge in its Charter to "respond effectively…to all forms of threats, transnational crimes, and transboundary challenges," member-states have failed to effectively respond to cybercrime attacks and foster international cooperation in cyber-space (ASEAN, 2007, p. 8). This is due to *two* key regional hurdles: 1) the digital divide within ASEAN members; 2) lack of harmonization between domestic laws and international cybercrime conventions, notably the Budapest Convention.

1) The Digital Divide

ASEAN is characterized by high levels of heterogeneity in terms of economic development, which is reflected in the varying degrees of maturity in ICT (Noor, 2020). This is conceptualized as the "digital divide" (OECD, 2001, p. 4) — a divide "between governments, businesses and geographic areas at different socio-economic levels with regard to their opportunities to strengthen information and communication technologies (ICTs)" (Shackelford & Craig, 2014, p. 122). This divide can be explained by the presence of three distinct silos observed within ASEAN.

The first, Silo A, includes states that have clearly internalized the issue of cybercrime and the threats that it poses to the socioeconomic potential of cyberspace (Tran Dai & Gomez, 2018). Members of Silo A, such as Singapore and Malaysia, reflect this internalization and prioritization of the benefits offered by a secure cyberspace. Singapore, for instance, acknowledges that disruptions caused by malicious actors have a detrimental effect on economies. This is largely because Singapore is an international center of exchange and commerce and, on balance, is more likely to invest significantly large proportions of their GDP (0.22%) into improving its cybersecurity posture compared to others within the ASEAN region (Tran Dai & Gomez, 2018). Through a multi-million dollar ASEAN Cyber Capacity-Building Program, Singapore has invested resources in launching new initiatives, including a drowning detection system, an open API-driven framework mobile apps to access government services to prevent attacks on systems that run utility plants, transportation networks, hospitals, and other essential services — in other words, to prevent attacks on the systems of industries that are vital to maximizing the socioeconomic potential of cyberspace (Noor, 2020; Tran Dai & Gomez, 2018). Similarly, according to Malaysia's National Cyber Security Agency, a secure infrastructure will "promote stability, social well-being and wealth creation" (Tran Dai & Gomez, 2018, p. 16).

The second, Silo B, comprises those member-states which recognize the presence of cybercrime threats, but may have various *competing* priorities, resulting in limited allocation of resources to tackle cybercrimes (Tran Dai & Gomez, 2018). Initiatives proposed by member-states in this group do not amount to an authentic reckoning with the magnitude of cybercrime and the necessity of tackling it to secure the cyber domain. For instance, although Vietnam acknowledges its susceptibility towards cybercrime threats via its 2015 Cyber Information Security Law. The state still appears torn between protecting its cybersecurity infrastructure on the one hand versus enforcing content control over their citizens' internet activities on the other (Tran Dai & Gomez, 2018).

Member-states in Silo B also invest significantly less in cybersecurity (0.03% of GDP) compared to those in Silo A (0.22% of GDP) as well as the global average (0.13% of GDP) (Tran Dai & Gomez, 2018). Less investment is attributed to the various competing issues on these states' policy agendas. Cybersecurity initiatives often compete with national infrastructure projects (e.g., schools, hospitals, roads) which often take priority in national budgetary allocations (Tran Dai & Gomez, 2018). The characteristics of states in Silo B evince a superficial similarity with those in Silo A regarding the importance of protecting the national cybersecurity infrastructure, though their observed actions suggest otherwise.

Thirdly, in Silo C, member-states do not recognize the gravity of cybercrime threats due to the absence of assets that are placed in harm's way, rather than due to the issue of diverging priorities (as in the case of Silo B) (Tran Dai & Gomez, 2018). This is typical of states that have *yet* to benefit from the digital economy and are in the infancy stages of working towards fulfilling the socioeconomic potential of cyberspace (Tran Dai & Gomez, 2018). Whereas, Silo A states simply aim to *maintain* that potential for they are already past the stage of fulfilling it. This is evidenced by the different rates of Internet access between states in Silo A versus states in Silo C. For instance, an average of 70.83% of Silo A's typical population have access to the Internet (Erksine & Carr, 2016). In contrast, only 24.17% of Silo C's states enjoy the socio-economic benefits of Internet access (Erkskine & Carr, 2016). This is largely the case with Cambodia, Laos, and Myanmar. Cambodia has developed a national Computer Emergency Response Team (CamCERT) which is tasked with awareness and outreach missions, digital authentication, and incident reporting. Within a span of six years, Laos has also been able to transform itself from having no national CERT into establishing its very own LaoCERT. Myanmar's Ministry of Communications and Technology, the country's primary ICT and cybersecurity institution, houses the national mmCERT tasked with incident handling and security advisory.

Despite these achievements, they face multiple challenges in equalizing their cyber-capabilities, including limited human resources and financial wherewithal to subsidize ICT infrastructures, as well as undeveloped cybersecurity awareness among the population. To develop an international cooperation framework by which all ASEAN members can collectively adopt, differences in levels of cyber-maturity, policy priorities, and levels of socioeconomic development between Singapore and Malaysia versus other member-states must be reconciled.

2) Lack of Harmonization

Relatedly, the digital divide has produced differing priorities between member-states which have subsequently hampered efforts to harmonize their domestic cybercrime laws with international ones. The Budapest Convention, recognized as the first and only international convention that deals with cybercrime, has not been signed or ratified by any of the ASEAN member-states (Broeders & van den Berg, 2020). This Convention aims to fast-track collaboration among states in cybercrime investigation and prosecution, while also aiming to facilitate the adoption of adequate legal instruments against cybercrime via both substantive and procedural parts of regulation — that is, by requiring signatories to criminalize offences against data confidentiality and integrity, such as illegal access, interception of non-public transmission, interference with computer data, and misuse of computer-related devices (Broeders & van den Berg, 2020). Enshrined under the Budapest Convention is the principle of international cooperation which requires signatories to extensively cooperate with each other, and to utilize a network of national or regional contact points such that any obstacles to the rapid flow of information are minimized "to the widest extent possible" (Broeders & van den Berg, 2020, p. 46). With that said, however, most ASEAN members — except Cambodia, which is still in the process of drafting its first national cybercrime law — have enacted domestic legislation to regulate cybercrime whose objectives are, *in theory*, aligned with those of international conventions (e.g., the Budapest Convention) (Tikk & Kerttunen, 2020).

In practice, however, most ASEAN governments prioritize the growth of the digital economy over developing the capacity-building measures required to bolster the region's cyber-maturity. For example, the ASEAN ICT Masterplan (2020) insists on "Initiative 8.1: Strengthen[ing] Information Security in ASEAN, creat[ing] a trusted ASEAN digital economy" (p. 26), which emphasizes the development of critical information infrastructures and the budgeting needed to develop them. According to Broeders and van den Berg (2020), aiming to narrow the "digital divide", the heads of ASEAN states agreed at the East Asia Summit in 2018 to foster cooperation:

> Promoting sustainable economic growth and prosperity, by supporting digital economy initiatives including investment and innovation, entrepreneurship, assisting Micro, Small and Medium Enterprises (MSMEs) to utilize ICTs and participate in the digital economy, developing a digital-ready workforce, and raising awareness of security in the use of ICTs. (p. 145)

Having demonstrated efforts to drive the growth of the digital economy, the issue of cybercrime has in essence become subsumed by "the larger priority of creating access to human resources and infrastructure capacity for the combined population" of ASEAN to capitalize on the promises of the Internet (Noor, 2020, p. 35).

ASEAN'S Cooperation Approach to Cybercrime: A Case of "Norm Subsidiarity"

As a result of uneven capabilities (IV) to deal with cybercrime, the work done so far at the national level in implementing domestic legislation, launching CERTs, and promoting the digital economy may not fully serve the global community, thereby delaying prospects for international cooperation.

To embody those cyber norms, which regulate state behavior along the lines of international cooperation, it is imperative to equilibrize the level of cyber-capabilities. Unable to do this, most member-states have instead resorted to "norm subsidiarity" — invocations of subsidiary norms — which determines the variation in outcome between that of ASEAN and the GCC.

To reiterate, Acharya (2011) defines "norm subsidiarity" as a "process whereby regional or local actors create rules with a view to preserve their autonomy" (p. 97). In the case of ASEAN, the purpose of "norm subsidiarity" is the invocation of regional norms which are integral to preserve their *autonomy* (Acharya, 2014). To put it in Acharya's words, regional groupings internalize "[cyber]norms by invoking and supporting a normative prior to securing their autonomy" (Acharya, 2011, p. 102). Some subsidiary norms located that are invoked and supported by ASEAN include a) non-intervention, b) consensus-based decision-making, c) preference for bilateral over multilateral cooperation, all of which have informed the "The ASEAN Way" of cybersecurity governance (Acharya, 1992; Acharya, 2014).

ASEAN's failure to equilibrize its cyber-capabilities is reflected in the region's strict adherence to the subsidiary norm of *non-interference* in internal affairs (Acharya, 2014). Although non-interference is generally viewed as a 'Westphalian' norm, this analysis shows how non-interference was regionalized

and specifically applied to Southeast Asia, giving rise to a non-Westphalian regional order. Given that most member-states, except for Thailand, were newly independent developing countries upon the creation of ASEAN, non-interference became the mainstay of intra-regional relations (Acharya, 2014). The salience of this norm in cyberspace has to be understood in the context of the organization's search for internal security. As Myanmar embroils itself in conflict between government forces and the Karen National Union, as the Cambodian government continues to control web traffic by censoring independent media outlets, and as Vietnam similarly conducts control over its Internet space, such domestic issues can be aggravated by foreign cyber-criminals, including interference from close neighbors. At any time, domestic sources of insecurity can generate a spillover effect on interstate relations. This would have a debilitating impact on possibilities for fostering *regional* cooperation. According to ASEAN, no framework for cooperation could be sustainable unless the group agrees on the fundamental importance of regional autonomy anchored in the principle of non-interference in national affairs (Acharya, 2014).

Another subsidiary norm invoked by ASEAN members is *consensus-based decision making* (Acharya, 1992; Acharya, 2014). This requires that member-states agree on a set of collective expectations regarding cyberspace. However, there is a potential for member-states to adopt expectations simply for the sake of consensus or because it would be strategically unwise to renegotiate that consensus. An ingenuine adherence to expectations may undermine the region's ability to avoid repeated cybercrime attacks, especially where attribution of those attacks remains challenging (Acharya, 2014).

Preference for short-term *bilateral* cybersecurity cooperation over long-term multilateral cooperation is another subsidiary norm invoked by ASEAN (Acharya, 2014; Heinl, 2014; Tikk & Kerttunen, 2020). On a bilateral basis, Singapore has signed individual Memoranda of Understanding with Australia, France, India, the Netherlands, the United Kingdom, and the United States as well as a Memorandum of Cooperation on Cybersecurity with Japan (Tikk & Kerttunen, 2020). It has also signed a Joint Declaration on cybersecurity cooperation with Germany (Tikk & Kerttunen, 2020). Another example is Laos which has sent the LaoCERT to join bilateral cybersecurity initiatives with Japan in 2012, as well as to sign cooperative agreements with other CERTs in the region, such as ThaiCERT in 2013, ID-SIRT (Indonesia) in 2015, VNCERT (Vietnam), and CNCERT (China) in 2017 (Tikk & Kerttunen, 2020; Zeng et al., 2017). Myanmar has also extended cooperation with Singapore to develop its cyber capabilities and participated in cyber training through the Myanmar-Singapore Training Compendium (Tikk & Kerttunen, 2020). Thus, ASEAN

governments have prioritized bilateral forms of cooperation to preserve their regional autonomy rather than engaging with the global system and coming in full support of a multistakeholder cybersecurity governance approach.

However, restricting ASEAN to bilateral governance approaches can ironically foreclose possibilities for cooperation even though they are invoked to deepen cooperation. This is because any intransigence by *some* member-states to coordinate with supranational organizations in multilateral forums, coupled with major variations in cyber-capabilities and the lack of compliance mechanisms, means that most decisions taken at the bilateral level depend on their effective implementation at *national* levels (Broeders & van den Berg, 2020; Noor, 2020). Cambodia, Laos, Myanmar, and Vietnam represent precisely the member-states states for whom superpower-centric multistakeholder cybersecurity dialogues are relevant but still rather foreign. Resilient ICT infrastructures cannot be achieved by directly focusing on strategic dialogue with cyber superpower states. In this respect, mobilizing ASEAN member-states around a common set of norms to foster international cooperation may prove challenging.

Cumulatively, these three subsidiary norms form the brick-and-mortar philosophy of ASEAN's cybersecurity governance approach: *The ASEAN Way*. This cooperation approach has leaned towards respecting the non-interference of member-states' national affairs, consensus-based decision-making in cyberspace, and informal institutional mechanisms including memoranda, declarations, statements, bilateral plans, and other loose cooperative mechanisms to maintain regional autonomy.

Therefore, uneven cyber-capabilities within ASEAN have led to an embodiment of norms consistent with *national/regional* cooperation (subsidiary norms) rather than *international* cooperation; also, that the cooperation approach of most ASEAN states is concentrated at the regional level represents an unwillingness to resort to great-power security guarantees and Western security orientations. This is why it does not fall under cyber-sovereignty or multistakeholder approaches.

The GCC's Regional Hurdles

The GCC confronts two regional hurdles in attempts to foster international cooperation in cyber-space—1) the digital divide; 2) lack of harmonization between domestic laws and international cybercrime conventions, notably the Budapest Convention — though to a more *limited* extent than ASEAN member-states.

1) Digital Divide

The GCC's current digitization levels reveal that cyber-capabilities between member-states are relatively *even* (Hakmeh, 2017). The importance of equalized cyber-capabilities within the region cannot be emphasized enough, given that all member-states are currently working to diversify their economies towards knowledge-based ones in order to reduce their reliance on oil rents (Hakmeh, 2017). A failure to tackle cybercrime would, therefore, compromise the region's strategic development visions.

Notwithstanding their streamlined cyber-capabilities, a phalanx of opinion, nevertheless, suggests the existence of a digital divide in the region (Kshetri, 2016; Lewis, 2014; Shires, 2019). GCC member-states still experience variations within cybersecurity preparedness — that is, the extent to which the member-states have developed the digital technologies that contribute to their "readiness to respond to or recover from a cybercrime attack" (International Telecommunication Union [ITU], 2018, p. 76). According to a 2018 McKinsey report, Saudi Arabia is the most digitally advanced among the GCC member-states in its cybersecurity-preparedness, while Oman and Qatar scored second and third respectively by a close margin (as cited in Shires, 2019). Although the UAE was assigned the top score in 2017, it was re-assigned to fourth place in 2018 (Shires, 2019). Meanwhile, Kuwait and Bahrain lagged behind the curve in terms of cyber-security preparedness. The scores assigned by McKinsey were also consistent with the ITU GCI's rankings, which measured their cybersecurity preparedness based on a combination of 25 indicators among the member-states (ITU, 2018). Saudi Arabia ranked the highest with a score of 0.881, followed by Oman (0.868), Qatar (0.860), UAE (0.807), Kuwait (0.600), and Bahrain (0.585) (ITU, 2018).

Based on these rankings, it would be reasonable to situate Saudi Arabia, Oman, Qatar, and UAE within Silo A, given that they have clearly internalized the issue of cybercrime and the threats that it poses to the socioeconomic potential of cyberspace. Added to this are the stakes involved in effectuating the necessary transitions within their respective economies (Kshetri, 2016). For example, Saudi Arabia has focused its investments on establishing a variety of institutions to combat emerging cybercrime threats, including a Computer Emergency Response Team (CERT), a National Cybersecurity Center (NSC), and a National Cybersecurity Authority (NCSA) (Shires & Hakmeh, 2020). The NSCA draws from the authority of government officials within existing security, defense, and intelligence ministries to integrate a multi-sector coordination in cybersecurity (Shires & Hakmeh, 2020). The NSC and NCSA are specifically tasked with conducting cyber-research and development — a sector which is recognized for

its socioeconomic potential and is estimated to reach a value of $3.4 billion (Shires & Hakmeh, 2020).

Similarly, Qatar has sent government officials to international cybersecurity events, consulted with cyber experts around the world regarding international cooperation in cyberspace, and called for the implementation of a standardized platform through Interpol to "enhance communication and cooperation" within cybersecurity (Shires, 2019, p. 237). Through its CERT, Oman was able to successfully deter 880 million cyber-attacks which targeted the country in 2017 (Shires, 2019). Oman has also exhibited immense interest in areas of international cooperation by referring its representatives to numerous international cybersecurity fora. Muscat is home to the ITU's Middle East Regional Cybersecurity Center, which pulls from the expertise of cybersecurity experts who collaborate on cybersecurity initiatives (Efthymiopoulos, 2016). The UAE has also poured its investments into the development of a CERT, a National Electronic Security Authority, and a cybersecurity center in Dubai (Efthymiopoulos, 2016). It has further allocated large portions of the national budget towards increasing cyber measures within a project to double spending on homeland security by 2024 (Efthymiopoulos, 2016). To further mature as a security actor, the UAE has displayed ambition in collaborating with international institutions to train the next generation of cyber experts.

Contrastingly, Kuwait and Bahrain share similarities with states in Silo B — those states which acknowledge the presence of cyber vulnerabilities yet have to manage competing priorities. They must balance between the need to boost their cybersecurity preparedness and the need to cope with other demands in their countries' infrastructure. This makes them slower than member-states in Silo A in adequately addressing the relative threats posed to its cybersecurity infrastructure.

2) Lack of Harmonization

Akin to ASEAN, the GCC's domestic legal frameworks on cybercrime are not harmonized with the Budapest Convention (Hakmeh, 2017). The GCC is currently not party to any international anti-cybercrime agreement. However, a cooperation framework exists at the regional level in the form of the Arab Convention on Combating Information Technology Offences (the 'Arab Convention') (Hakmeh, 2017). This regional cooperation framework was signed in 2010 by all GCC states — other than Saudi Arabia — with the objective of improving cooperation between member-states to "combat information technology offences threatening their security, interests and the safety of their communities" and enabling State Parties to "adopt a common policy aimed at

protecting Arab society against information technology offences" (Hakmeh, 2017, p. 11).

Harmonization is integral to foster international cooperation to tackle cybercrime. It is one thing to have domestic cybercrime laws, and quite another to bring those domestic legal frameworks in express alignment with an international cybercrime convention which can, in turn, provide the basis for moving beyond regional cooperation towards *international* cooperation. Although it has not signed the Budapest Convention, some scholars such as Hakmeh (2017) and Shires (2019) argue that the member-states' domestic cybercrime laws have codified the principles and values entrenched in Article 15 of Convention, namely, procedural powers, international cooperation, and human rights values in cyberspace.

However, other scholars contend that the codification of such principles and values are tokenistic at best (Eggenschwiler, 2018). Most of their domestic laws focus on criminalization of cyberattacks and broadening the definition of content-related cybercrime to a range of acts such as defamation, sedition, and damaging the state's reputation via political speech online — that is, using ambiguously worded provisions which may, therefore, fail to ensure "the adequate protection of human rights" in cyberspace (Eggenschwiler, 2018, p. 74). Their domestic laws are, thus, a combination of direct influence from the original text, as well as additions that appropriate principles from the Budapest Convention and repurpose them to cover political speech online (Eggenschwiler, 2018).

GCC national cybersecurity strategies generally include only an abstract description of measures taken to tackle cybercrime. For example, the Bahrain strategy claims to "establish a secure cyberspace to protect the Kingdom of Bahrain against cyber-threats to reduce risks" (Hakmeh, 2017, p. 18). The Qatari strategy presents "an integrated and holistic approach that will enhance synergies and cooperation, avoid duplication, and maximize resource utilization in managing the dynamic environment and emerging threats in cyberspace" (Kshetri, 2016, p. 182). In Dubai, "the goal is to build a more secure information society that is perfectly aware of cybersecurity risks", whose key objectives are to "address any risks, threats or attacks" (Hakmeh, 2017, p. 22). Saudi Arabia's strategy also aims to construct "an effective and secure national information security environment" (Kshetri, 2016, p. 185).

GCC's Cooperation Approach to Cybercrime: A Case of "Norm Diffusion"

Unlike ASEAN which favors neither cyber-sovereignty nor multistakeholderism, the cybersecurity strategies of GCC member-states represent a unique case since

it assumes a *hybrid* position between these two camps (Shires, 2019). It is this *hybrid* position through which GCC member-states are increasingly able to *diffuse* norms vis-à-vis international cooperation. "Norm diffusion" is the process wherein norms are "socialized and shared, and then become internalized, accepted, and implemented" by national or regional actors (Acharya, 2011, p. 97; Taddeo, 2018).

On the one hand, the GCC states' authoritarian tendencies might place them in a similar category as China, Russia, and other supporters of cyber-sovereignty. The GCC states, for instance, have similar outlooks with China and Russia on the control of national information, e.g., via censorship of political speech, as exemplified by the states' expansion of cybercrime to cover political speech under their domestic cybersecurity laws. According to Bronk and Tikk-Ringas (2013), these domestic cybersecurity laws breach internationally recognized rights to freedom of expression.

On the other hand, unlike China and Russia, the GCC states also have extensive security relationships with Western liberal democracies that uphold multistakeholder values (Shires, 2019). The Gulf's cybersecurity and intelligence relationships are closely aligned with the United States and Europe. For example, the United Kingdom's covert surveillance program "CIRCUIT" depends on Oman for signals intelligence collection on Iraq and Yemen, while Saudi Arabia and the UAE are approved Third Parties who have some access to the US National Security Agency's signals intelligence (Shires, 2019, p. 237). As well, there exists a UK-Saudi Arabia Joint Communiqué to develop strategic cooperation to combat cybercrimes (Shires, 2019). Beyond state-to-state relations, European and US-based companies have sold an array of defensive cybersecurity solutions and security consultancy services to most major companies and government agencies in the GCC (Shires, 2019). Finally, the GCC has consistently pursued international cooperation with the UK and the US through meetings in which both sides have agreed to increase information-sharing on cybersecurity initiatives to counter Iran's cyber-aggression — a phenomenon which has posed concerns for both the US and the GCC states. Within these meetings, Ibrahim Al-Shamrani, Executive Director of Operations at Saudi Arabia's National Cybersecurity Center, expressed that although GCC states cooperate on cybersecurity at the regional level, they "cannot work alone," thereby signifying Saudi Arabia's interests in international cooperation efforts (Shires, 2019, p. 236).

The fact that the GCC has been able to facilitate cybersecurity partnerships with the UK and US provides significant explanatory power for the region's high rankings on the ITU's *multistakeholder* cooperation pillar (ITU, 2018). They

were ranked according to measures based on the existence of international partnerships, cooperative frameworks and "multistakeholder approach[es] with inputs from all sectors" (including multilateral agreements, participation in international fora, public-private partnerships, inter-agency partnerships) (ITU, 2018, p. 9). According to the ITU framework, Saudi Arabia and Oman were both ranked the highest (0.160) in the Arab region for facilitating "international multistakeholder cooperation in cybersecurity," alongside Qatar (0.151) (ITU, 2018, p. 7). Due to these practices, the GCC states cannot simply be cast as cyber-sovereign or as spoiler forces against multistakeholderism.

As mentioned earlier, the lack of harmonization, coupled with corresponding *ambiguities* in domestic cybercrime legislation, represented a regional hurdle for fostering attempts to tackle cybercrime threats. According to scholars such as Shires & Hakmeh (2020), since the GCC has yet to clarify those legal ambiguities, the scope of discussion on international cooperation will remain limited. However, this paper argues that those discussions are not completely foreclosed. In other words, ambiguous domestic cybersecurity laws have enabled GCC states to *diffuse* international cyber norms while avoiding ideological disagreements that could potentially jeopardize efforts towards cooperation. What was initially a hurdle later became an opportunity by which the GCC member-states used to maintain their hybrid position. That hybrid position — via extensive cybersecurity partnerships with advocates of both cyber-sovereignty and multistakeholderism — subsequently widened attempts for member-states to *diffuse* cyber norms in the international system.

Ambiguity is a common theme of international politics both within and outside the cybersecurity domain (Erksine & Carr, 2016). There are various degrees of ambiguity in IR discourse, some of which are not purposeful — given that ambiguity can purely result from rapidly changing circumstances or lack of knowledge in cyberspace — though other ambiguities are *deliberately* cultivated (Shires, 2019). According to IR scholar Seabrooke (2014), rather than simply importing Western expert knowledge and best practices on cybersecurity, security actors can conduct epistemic arbitrage, a process whereby these actors "mediate between [various] knowledge pools for strategic advantage" (p. 54). The process of epistemic arbitrage is inherently ambiguous and flexible because security actors can shift between "theoretical wrangling and ad hoc application" depending on its strategic needs (Seabrooke, 2014, p. 63). GCC member-states have strategic reasons for creating ambiguity. Rather than a hurdle, therefore, ambiguities within the GCC's domestic cybersecurity frameworks may be the eventual secret to its success in fostering international cooperation.

Plainly stated, GCC domestic cybersecurity laws *diffuse* relatively *abstract* norms based on human rights, individual freedom and privacy, though they are strategically packaged for international consumption. Within epistemic arbitrage, the GCC member-states capitalize on the abstract nature of these rights-based norms in order to package them to international audiences (Seabrooke, 2014). For instance, Saudi Arabia's cybersecurity strategy aims to "enable information to be used and shared freely and securely," while the National Cyber Security Center seeks to "realize a safe, open and stable information society" (Kshetri, 2016, p. 187). Similarly, the Dubai strategy stresses upon the importance of "a free and secure cyber world," claiming that "cyberspace needs to remain open to…the free flow of ideas, information, and expression," while "due consideration should be made to maintain the proper balance between open technology and the individual rights of privacy" (Hakmeh, 2017, p. 34). In a similar vein, both Qatar and Bahrain's strategies claim that their "norms and values in cybersecurity" are to "show tolerance, respect", and to "maintain the rights and values of individuals" (Hakmeh, 2017, p. 40). Such strategies constitute a tactical portrayal of abstracted Internet rights and freedoms to their international audiences (Shires, 2019).

Yet, the GCC's endorsement of ambiguous rights-based norms in cyberspace is *qualified* by references to safety and care. In Kuwait, "the strategy is primarily intended to promote the culture of cybersecurity which supports the *safe* and right use" of the Internet (Kshetri, 2016, p. 193). Qatar aims to "foster a culture of cybersecurity that promotes *safe* and appropriate use of cyberspace" (Shires, 2019, p. 238). In order to maintain careful use of social media, GCC member-states have constantly updated firewalls, password management systems, and *more importantly*, expanded the list of offences which constitute cybercrime within its legal frameworks to include political speech (Shires, 2019). The Dubai strategy, for example, explains that "fraud, terrorism, violation of privacy, and defamation" are offences which have interrelated links to cybercrime (Shires, 2019, p. 239). Under the GCC's domestic cybersecurity laws, the concept of cybercrime is effectively expanded to encompass to cover any category of political speech defrauding, terrorizing, or defaming the government online.

GCC's cybersecurity laws are fraught with "public morals" and appeals to ideas of "national unity," given the repeated emphasis on the citizens' role to maintain "the safe and appropriate use of cyberspace for all" (Shires & Hakmeh, 2020, p. 14). The Omani cybercrime law contains a section explicitly titled "cybercrimes," covering any use of ICTs to "produce or publish or distribute or purchase whatever might prejudice the public order or religious values" (Shires, 2019, p. 237). This means that many social media posts, including any political

opposition online, would be considered a cybercrime — for which there are strong penalties. Saudi Arabia's cybercrime law, for instance, has a "naming and shaming" clause for 'cybercriminals' which allows their name and details of their offence to be published in local newspapers (Eggenschwiler, 2018, p. 73). Similarly, Article 9 of the UAE cybersecurity law punishes almost any form of political speech "by temporary imprisonment and a fine not in excess of one million dirhams [to] whoever publishes information, news, statements, or rumors on any ICT with intent to damage the reputation, prestige and stature of the State, or national peace" (Efthymiopoulos, 2016, p. 14). Domestic cybercrime laws were therefore used to target political speech online, namely by political groups (e.g., the Al-Islah group were accused by the UAE government of affiliation with the Muslim Brotherhood), political dissidents (e.g., Nasser Bin Ghaith who was charged under the cybercrime law in 2016 for defaming the UAE government as well as Nabeel Rajab who had posted anti-government tweets in Bahrain), bloggers (who criticized Kuwait's emirs in 2016), social media accounts (spreading rumors regarding the alleged murder of Saudi journalist Jamal Khashoggi by the Saudi government in its Turkish consulate) (Eggenschwiler, 2018).

In all cases, the ambiguities of domestic cybersecurity legislation allowed the GCC states to maintain their hybrid position between *cyber-sovereignty* and *multistakeholderism*. Legal provisions of safe and right [Internet] use was strategically used by member-states to cooperate with other stakeholders (e.g. the UK) and prevent the spread of cybercrime in a way that secures human rights for all users in cyberspace (reminiscent of *multistakeholderism),* while also regulating political speech online (revelatory of *cyber-sovereignty* practices) which simultaneously risks violating those rights.

Conclusion

By comparing ASEAN and the GCC through a MSSD research design, it was found that the former is oriented towards the legitimization of *national* and *regional* cooperation in cyberspace (via "norm subsidiarity"). Whereas, the latter has converged their efforts around establishing mechanisms for *international* cooperation to tackle cybercrime threats (via "norm diffusion").

Overall, this project constitutes merely one small step towards unveiling the norm dynamics of non-Western regional organizations in cyberspace. While this preliminary research offers findings that are *internally* valid within Southeast Asia and the Persian Gulf, further research is needed to boost its *external* validity to other non-Western regional groupings. Since the sample of interest comprises two non-Western regional institutions with the most shared characteristics — in

terms of their institutional history, security orientation, geographic concentration of member-states, and degree of cultural *heterogeneity* and political *homogeneity* — it would be worthwhile to test the generalizability of this paper's findings by conducting other cross-regional comparisons between, for instance, ASEAN and another regional group within the broader universe of cases, such as the South Asian Association for Regional Cooperation (SAARC).

Given that both organizations consist of largely authoritarian states, future research should also examine whether the *distinct* norm dynamics in ASEAN ("norm subsidiarity") and the GCC ("norm diffusion") have opened further opportunity for cyber-authoritarianism during the COVID-19 pandemic. As highlighted earlier, due to the process of epistemic arbitrage within norm diffusion, GCC member-states have developed domestic cybersecurity laws that are ambiguously rights-based yet also include an expanded definition of cybercrime that stretches anywhere from advanced-persistent-attacks attacks to dissident speech. How have pandemic conditions, therefore, served as the justificatory basis for encroachment on civil liberties, increases in intelligence tracking, mass surveillance, and other technologies that support authoritarian governance in the Gulf? As ASEAN attempts to equalize cyber-capabilities in the region, how has norm subsidiarity enabled member-states to co-opt domestic technology industries to retain sociopolitical control and build cyber-capabilities as a means to bolster their legitimacy in the region? These questions are proposed with heightened urgency.

References

Acharya, A. (1992). Regional military-security cooperation in the third world: A conceptual analysis of the relevance and limitations of ASEAN (Association of Southeast Asian Nations). *Journal of Peace Research, 29*(1), 7-21. http://www.jstor.org/stable/423875

Acharya, A. (2011). Norm subsidiarity and regional orders: Sovereignty, regionalism, and rule-making in the third world. *International Studies Quarterly, 55*(1), 95-123.

Acharya, A. (2014). *Constructing a security community in Southeast Asia*. Taylor and Francis. https://doi.org/10.4324/9781315796673

Amirahmadi, H., & Entessar, N. (Eds.). (2002). *Reconstruction and Regional Diplomacy in the Persian Gulf*. Routledge.

Association of Southeast Asian Nations (ASEAN). (2007). *The ASEAN Charter*. https://asean.org/wp-content/uploads/images/archive/publications/ASEAN-Charter.pdf

Association of Southeast Asian Nations (ASEAN). (2020). *The ASEAN ICT Masterplan 2020*. https://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf

Barcomb, K. E., Krill, D. J., Mills, R. F., & Saville, M. A. (2012). Establishing cyberspace sovereignty. *International Journal of Cyber Warfare and Terrorism (IJCWT), 2*(3), 26-38.

Bartelson, J., Costa Lopez, J., De Carvalho, B., Latham, A. A., Zarakol, A., & Holm, M. (2018). In the beginning there was no word (for it): Terms, concepts, and early sovereignty. *International Studies Review*, *20*(3), 489-519.

Broeders, D., & van den Berg, B. (2020). Governing cyberspace: Behavior, power and diplomacy. In D. Broeders & B. van den Berg (Eds.), *Governing Cyberspace*. Rowman & Littlefield Publishers.

Bronk, C., & Tikk-Ringas, E. (2013). The cyber-attack on Saudi Aramco. *Survival*, *55*(2), 81-96.

Chandra, G. R., Sharma, B. K., & Liaqat, I. A. (2019). UAE's strategy towards most cyber resilient nation. *International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8*(12), 2803-2809.

Efthymiopoulos, M.P. (2016). Cyber-security in smart cities: The case of Dubai. *Journal of Innovation and Entrepreneurship*, *5*(1), 1–16. https://doi.org/10.1186/s13731-016-0036-x

Eggenschwiler, J. (2018). A typology of cybersecurity governance models. *St Antony's International Review*, *13*(2), 64-78.

Erskine, T., & Carr, M. (2016). Beyond 'quasi-norms': the challenges and potential of engaging with norms in cyberspace. In A.M. Osula & H. Rõigas (Eds.), *International cyber norms: Legal, policy & industry perspectives* (pp. 87-110). NATO Cooperative Cyber Defence Centre of Excellence.

Hakmeh, J. (2017). *Cybercrime and the digital economy in the GCC countries*. Chatham House.

Halperin, S., & Heath, O. (2020). *Political research: Methods and practical skills*. Oxford University Press.

Heinl, C. (2014). Regional cybersecurity: Moving toward a resilient ASEAN cybersecurity regime. *Asia Policy*, (18), 131-160.

Hemmati, M., Dodds, F., Enayati, J., & McHarry, J. (2002). *Multi-stakeholder processes for governance and sustainability: beyond deadlock and conflict*. Routledge.

Hofmann, J. (2016). Multi-stakeholderism in internet governance: Putting a fiction into practice. *Journal of Cyber Policy*, *1*(1), 29-49.

International Telecommunication Union. (2018). *Global cybersecurity index*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Job, B. (1992). The insecurity dilemma: National, regime, and state securities in the third world. In B. Job (Ed.), *The insecurity dilemma: National security of third world states*. Lynne Rienner Publishers.

Kshetri, N. (2016). Cybersecurity in Gulf Cooperation Council economies. In N. Kshetri (Ed.), *The quest to cyber superiority* (pp. 183-194). Springer International Publishing.

Lewis, J. A. (2014). *Cybersecurity and stability in the gulf*. Center for Strategic & International Studies.

Noor, E. (2020). Positioning ASEAN in cyberspace. *Asia Policy*, *27*(2), 107–114. https://doi.org/10.1353/asp.2020.0033

Organization for Economic Cooperation and Development. (2001). *Understanding the digital divide.* https://www.oecd.org/sti/1888451.pdf

Pawlak, P., & Barmpaliou, P.N. (2017). Politics of cybersecurity capacity building: Conundrum and opportunity. *Journal of Cyber Policy*, *2*(1), 123–144. https://doi.org/10.1080/23738871.2017.1294610

Perritt Jr., H. H. (1997). The Internet as a threat to sovereignty-thoughts on the internet's role in strengthening national and global governance. *Indiana Journal of Global Legal Studies*, *5(2)*, 423-442.

Seabrooke, L. (2014). Epistemic arbitrage: Transnational professional knowledge in action. *Journal of Professions and Organization*, *1*(1), 49-64.

Shackelford, S. J., & Craig, A. N. (2014). Beyond the new "digital divide": Analyzing the evolving role of national governments in internet governance and enhancing cybersecurity. *Stanford Journal of International Law*, *50*(1), 119.

Shires, J. (2019). Hack-and-leak operations: Intrusion and influence in the gulf. *Journal of Cyber Policy*, *4*(2), 235–256.

Shires, J., & Hakmeh, J. (2020). *Is the GCC cyber resilient?* Chatham House International Security Programme. https://www.chathamhouse.org/sites/default/files/CHHJ8019-GCC-Cyber-Briefing-200302-WEB.pdf

Taddeo, M. (2018). The limits of deterrence theory in cyberspace. *Philosophy & Technology, 31*(3), 339-355.

Tikk, E., & Kerttunen, M. (Eds.). (2020). *Routledge Handbook of International Cybersecurity.* Routledge.

Trachtman, J. P. (1998). Cyberspace, modernism, jurisdiction and sovereignty. *Indiana Journal of Global Legal Studies*, *5*(2), 561-581.

Tran Dai, C., & Gomez, M. A. (2018). Challenges and opportunities for cyber norms in ASEAN. *Journal of Cyber Policy*, *3*(2), 217–235.

Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of “internet

sovereignty". *Politics & Policy*, *45*(3), 432–464. https://doi.org/10.1111/polp.12202

Author Biography

Hanan Mohamed Ali is a Master of Arts candidate at Simon Fraser University's School for International Studies. She holds a Bachelor of Arts (Honours) degree in Political Science and History. Her research interests coalesce around non-Western cybersecurity architectures, norm-creation, and international cooperation. Her research also further seeks to examine the interstices between cyber-governance, gender, and (bio/necro) politics particularly in the context of COVID-19. She has presented in conferences, including the 2021 Graduate Student E-Conference at McGill University's Centre for International Peace & Security Studies (CIPSS), in collaboration with the Centre for International Policy Studies (CIPS) at the University of Ottawa.

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