Cyber Security in East Asia: Governing Anarchy

Dr Nicholas Thomas
Research Assistant Professor
Centre of Asian Studies
University of Hong Kong

> There is a pressing need to contain cyber-crime through international cooperation. Without effective…control it is impossible to develop a networked society that is secure, convenient and comfortable.[1]

> The internet is fast, whereas criminal law systems are slow and formal. The internet offers anonymity, whereas criminal law systems require identification of perpetrators…The internet is global, whereas criminal law systems are generally limited to a specific territory. Effective prosecution with national remedies is all but impossible in a global space.[2]

> We are stranded…between the inadequacy of the nation-state and the emerging imperative of the global community.[3]

Abstract

The 13 countries of ASEAN+3 are actively working towards creating a regional community in East Asia. While these community building endeavours have been designed to capture the synergistic potential latent in the thirteen countries, they have not been without their own perils and pitfalls. At the same time, as the regional countries have modernized they have increasingly relied on web-based technologies to enable them to more efficiently use their resources. Even as this adoption of technology has assisted regional states, it has exposed them to new threats; with a growing number of East Asian networks and users now subject to a wide range of cyber attacks. These attacks have occurred within and across national boundaries with the transnational nature of cyber security making it difficult for governments to unilaterally securitize emergent cyber threats. As a result, it is becoming increasingly necessary for East Asian governments to protect their interests by working together. To do so effectively will require the adoption of policies and processes used to foster regional integration in other sectors (such as economic or political cooperation) and transfer them into the realm of cyberspace.

Introduction

Since 1967 the countries of East Asia have been coming together to form a regional community.[4] While these community building endeavours have been designed to capture the synergistic potential latent in the thirteen countries, they have not been without their own perils and pitfalls. In 1997 the devaluation of the Thai Baht caused a speculative attack on other regional countries, endangering not only national financial and economic institutions but also substantially diminishing the wellbeing of citizens in the affected countries. The main lesson from the Asian crisis was that the growing

interdependence of the region had negative as well as positive ramifications. This was reinforced in 2001/02 when terrorist cells in Singapore and Indonesia sparked security alerts across East Asia. What now happens in the region has become the concern of all countries, not just those immediately affected. Indeed core regional institutions, such as ASEAN, ASEAN+3 and APEC, are now devoting more time and resources to addressing a myriad of common security concerns. Initially such security concerns revolved around economic and environmental issues; however, in the last five years, the set of security issues has expanded to also include terrorism, transnational crime and biological threats.

As the regional countries have modernized they have increasingly relied on web-based technologies to enable them to more efficiently use their resources. However, this virtual process has mirrored the uneven pattern of economic development found across East Asia.[5] Thus states such as Japan, South Korea and Singapore are markedly more technologically advanced than other states such as China, Indonesia, Malaysia, the Philippines and Thailand, but even these are significantly more advanced than countries such as Brunei, Cambodia, Laos, Myanmar or Vietnam. However, the infrastructure in all but the first set of regional countries is rudimentary compared to the more developed states of Europe and North America. While this "digital divide" is often discussed in terms of economic development, the technological disparities and low resource capacity levels also presents a significant security challenge to these states, as well as all others linked to the World Wide Web (hereafter simply web).

The need to respond to this security challenge can be seen from the increasing exposure of East Asian networked users to cyber attacks. In Japan, for example "the number of cyber-crimes uncovered by police in 2004 increased 13 percent from the previous year to 2,081", with the figure more than doubling over the past five years.[6] The following year reports increased 52 percent to 3,161 reported incidences.[7] While, in South Korea, in 2002 the number of internet-based criminal cases increased to 60,000 up from 121 in 1997.[8] By 2006 it had increased to 70,545 instances, with identity fraud and hacking being the two most prevalent crime types.[9] Although this jump was undoubtedly due, in part, to the effects of new legislation it does reflect a genuine upwards trend in cyber crime reports; a trend that is evidenced in other regional countries as well as in extra-regional jurisdictions. In addition to the increase in cyber threats, the nature of the threats is also changing as cyber groups become more sophisticated in the structure of their attack vectors. As Stone stated, "These range from elaborate 'phishing' scams, which use phone web sites to steal credit card numbers and perpetrate identity theft; fraudulent spam that launches viruses or spyware; and 'malware' such as Trojans, which enable criminals to take remote control over thousands of computers for massive, distributed attacks."[10] With respect to the last item on Stone's list, it is worth noting that for the first half of 2007, China accounted for 29 percent of all global bot attacks, up from 26 percent in the same period in 2006. China also ranked second (behind the United States) for all forms of malicious computer activity in 2006.[11] As China's online presence grows these will be issues of concern not only for China but also for other countries exposed to its web presence.[12]

This paper presents a review of attempts to regulate and prevent cyber security threats in East Asia. This analysis is undertaken at the three levels: domestic, regional and international. It is suggested that the transnational nature of cyber security makes it difficult for governments to unilaterally securitize emergent threats from cyberspace.

Instead, it is necessary for Asian governments to protect their interests by working together at the regional level. Moreover, given the nature of cyberspace, such cooperation cannot be undertaken without due reference to what is going on in other parts of the world; especially the more technologically advanced countries and regions. Thus, in order to properly contextualize these efforts and provide appropriate policy suggestions, a framework that transcends international-domestic (intermestic) boundaries is required. For the purposes of this paper an intermestic structure will be adopted to frame the three levels of analysis. Before concluding this paper will explore the implications arising from this review and put forward possible areas for policy development.

The Securitization of Cyberspace

The Westphalian system had only been in existence for just over 320 years when the first Internet connection was made.[13] Prior to 1969 a state-centric structure that presupposed security as being an integral part of the state system was in force. Over the following thirty years the web came into its own as a critical medium for governance, commercial exchange and social interaction; although it has only been in the post-1990 period that this development has produced meaningful results, while also generating to significant challenges to state security. The decentralized and unregulated nature of cyberspace meant that it was a medium quasi-separated from the traditional scope of state security. Thus, even though "most of the period since 1945…the international system was both defined and maintained by the rivalry of two superpowers and their respective alliances",[14] the creation of cyberspace reflected the appearance of a more fluid international system; one where non-state actors, social groups or even individuals could materially affect the system's stability. It is ironic that a creation designed to ensure the survival of the state in the event of a massive attack on its essential infrastructure has itself become a potential vehicle for just such an attack.

At the same time as the web was coming of age international norms were also being reconsidered as new international structures and power balances began to evolve. As Risse-Kappen stated, "The end of the Cold War and the dissatisfaction with prevailing approaches to international relations…opened new spaces for theorizing about world politics".[15] This evolution in international relations led to search for a new security doctrine that could better explain the overlapping nature of nation-state's various interests; one that could reconcile the traditional challenges facing states with non-traditional threats such as international economic instability or global environmental degradation.

One of the new issues to be considered concerned the nature of the relationship between state sovereignty and security, in particular the ways in which threats could spread from the domestic realm to the international, and visa-versa. Such interdependence suggested an overlapping of state needs with other states' policies and practices and/or with activities within the international realm. The mutual dependence that such threats created affected not only states but also their attendant markets and societies. The space where the international met the domestic was fluid, depending on the type of issue that was crossing the boundaries and the concomitant responses that were required. The fluidity of such intermestic issues is especially apparent when

considering the different types of security threats that have gained prominence in the post-Cold War period.

In this period more attention has been paid to non-traditional security threats – in other words, threats that may emanate intentionally or otherwise from one nation-state to challenge the security of another nation-state. In 1994, the UNDP released its annual report entitled *New Dimensions of Human Security*. Although developmentally-focused this report categorized a broad range of non-traditional security threats within seven interdependent groups, namely: economic security, food security, health security, environmental security, personal security, community security, and political security.

It is interesting to note that the Internet and the web were still too limited to be included in this report.[16] Later Buzan, Wæver and de Wilde also listed a range of sectors from which threats could emerge.[17] These encompassed the military, environmental, economic, societal and political sectors. Again cyberspace was overlooked. Yet in the contemporary period the potential for virtual realm of cyberspace to be used as a conduit to harm those in the real world is seen as one of the most serious threats to national stability and prosperity. As the 2003 *National Strategy to Secure Cyberspace* stated with respect to the United States:

> Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security…Because of the increasing sophistication of computer attack tools, an increasing number of actors are capable of launching nationally significant assaults against our infrastructures and cyberspace.[18]

Securitization as an analytical tool was first propounded by the Copenhagen School (led by Buzan and Wæver). It describes a process through which an issue becomes considered a security threat and the policy actions that are then undertaken to alleviate or mitigate its impact. This process is characterized by a "speech act" whereby a threat is identified to a referent object by a securitizing actor. The actor succeeds in securitizing the issue when a target audience is convinced. Once this is achieved, the securitizing actor can then undertake certain emergency actions outside of normal political processes to address the threat. An identified threat may also be "desecuritized" as the securitizing actors seek a return to politics as normal.[19] This reverse process can occur either through the threat being downgraded or addressed. It is, however, usually an indirect process "where a shift of orientation towards other issues reduces the relative attention to the previously securitized issue."[20] This raises the question as to who securitizes an issue? With respect to cyberspace a variety of actors can be readily identified has having successfully securitized issues in the past. These include from governments to corporations to cybersecurity specialists and computer programmers. Examples of issues these actors have securitized encompass alerts to network and software vulnerabilities, virus alerts and reports on cyber criminal activities. In all these cases, the issues become securitized as these actors are considered by a broad spectrum state, market and social entities to be sufficiently informed on potential threats from cyberspace.

From the preceding discussion it is possible to conceive of a spectrum of threat responses that range from political solutions to securitized solutions. Beyond securitized solutions one may also consider militarized solutions, when even emergency mode responses by securitizing actors prove insufficient to alleviate the threat. At the opposite

end of the spectrum it may also be possible to discuss these issues in terms of social challenges that subsequently become politicized. In each case there is a need for an actor to successfully securitize an issue by convincing a significant cohort of the existential threat to their wellbeing.

However, while the Copenhagen School may consider a speech act to be a sufficient indicator of securitization, it is necessary to take into account other factors when exploring securitization. Although a securitizing actor may declare an issue a threat, it is necessary to consider the second stage of the response; namely the allocation of resources to alleviate or mitigate the threat. It is also important to evaluate how efficiently and how quickly the resources are allocated.[21] In other words, it is one thing to declare an emergency, but the securitizing actor has to also undertake actions that signal a shift from a normal political mode to an emergency mode. Without this second stage of evaluation it is not possible to understand if an issue has been securitized or if a rhetorical statement has merely been declaimed without substantive effect.

In East Asia, this second stage can be difficult to detect; primarily because the definition of what constitutes "normal" political behaviour is not readily apparent in most nation-states. This is even more of a problem when the liberal European-centric nature of securitization is theoretically grafted onto regional political systems; a significant number of which remain illiberal (encompassing communist systems, monarchies, authoritarian regimes or failed states). It also needs to be considered that many regional countries are still emerging from the decolonisation phase of development and are therefore either (a) resistant to defining issues as threats, as such a move may give rise to questions of state legitimacy or, conversely, (b) may seek to securitize issues that are not security threats in an effort to strengthen the state regime. Furthermore, if securitization is defined primarily as a shift in resources to meet a threat condition then the low surplus capacity prevalent in many regional states may constrain their ability to shift substantively into emergency mode even when such a threat is clearly identified.

The second point can be identified in more developed countries, but the first point is more likely to be a factor where nation-states lack liberal plurality. As noted above, this is a particularly relevant issue in the East Asian region. It is possible to hypothesize that in dealing with the securitization of threats in East Asia there may be a gap between the threat, its identification by a securitizing actor, and the mobilisation and deployment of resources to mitigate it. It can therefore be hypothesized that states – as the main securitizing actors in the region – will prefer to seek alternate political strategies to addressing a threat so as not to weaken their legitimacy before moving to fully securitize it. As such, when East Asian states do choose to securitize a cyber threat it can be seen as either a reaction to a public policy issue or in response to regional or international pressures.

The securitization of cyberspace is one of the more difficult responses to an emergent threat undertaken since the end of the Cold War. Unlike other issues – the environment, health or political rights – cyberspace is not coterminous with national borders. It is a disaggregated realm where different components of the threat and its response can be spread across multiple boundaries and where regulation is still the exception rather than the rule. Further, the fact that a virtual threat has been actualized may not be properly understood until after the event, given that non-human units can be the target (such as electronic bank accounts) and may not actually be materially affected

(as occurs when documents are only copied – rather than transferred or deleted). Moreover, as cyber threat are quite new and represent a hitherto unknown security threat it may not be possible to immediately conclude that it has been securitized, as a completely new set of resources have to be allocated to deal with it. This last point would be more relevant to countries that have only recently (or are still imperfectly) integrated with the web – an accurately portrayal of most East Asian states. All of which makes developing effective tools to analysing the securitization of cyber threats highly problematic.

Cyber threats can be divided into three categories: cyber crimes, cyber security, and cyber warfare. For the purposes of this paper only the first two will be examined (with a focus on the second category) as cyber warfare is a strategic rather than security issue. Nonetheless the three categories can be seen as lying on a spectrum of cyber threats that use similar methods but with differing vectors and intent – from the relatively micro-scale cyber crimes to macro-level cyber strikes against critical national infrastructure – and hence are partially synonymous with each other. For the purposes of this paper cyber crimes will be defined as criminal acts that (a) makes use of web-based technologies and (b) whose initiator/s and victim/s are within the same domestic realm. Cyber security threats will be defined as having an implicit transnational nature – where the initiator/s and victim/s are in separate nation-states – which rely on web-based technologies to undertake the harmful act. Such acts can be criminal (such as extortion)[22], destabilising behaviour (an actor within a nation-state affecting the operations of another actor from another nation-state, such as that which occurred in April 2005 between Chinese and Japanese groups and organizations)[23] or simply malicious (as in the release of harmful programs, for example, the "I Love You" or "Melissa" viruses).[24] In contrast, cyber warfare is an attack by a state or states or state-sponsored groups against another state or states through the use of web-based technologies, that may or may not be part of a wider strategic threat (for example, the 1998 "Moonlight Maze" attack against the US Department of Defence or the 2003 – and later – "Titan Rain" attacks by Chinese actors against US, UK and German strategic and commercial interests).[25]

The challenge posed by cyber threats becomes more complex when examining issues of cyber security as the threat initiator or recipient can be highly disaggregated, thus making the task of establishing a sufficiently representative audience far harder. In cyberspace cross-border threats can be targeted at corporations, social organizations or individuals as well as state units by other corporations, social organizations, individuals or states from any other part of the world. Further, coalitions can be developed between any of these units – either within the same territory or across additional boundaries – to enhance the threat potential or to diminish it. As McCusker (quoting the Council of Europe) has noted '[c]ybercrime requires less control over a geographical territory, less violence and intimidation, less personal contacts and thus less relationships based on trust and enforcement of discipline between criminals, in short less need for formal organisations.'[26]

Hence, securitizing actors on matters of cyber security tend to be larger referent units with pre-existing constituencies (such as states, international organizations, transnational and national corporations) or smaller units with representative status with these larger units (such as internet security organizations and some civil society

organizations). Individuals or groups without representative legitimacy find it far more problematic to securitize an identified threat. As noted above, in East Asia, with a predominance of illiberal regimes, the securitizing actors are frequently the state regimes; although regional and international organizations can and do exert significant influence on state behaviour in this area.

East Asian Responses to Cyber Threats

Given this highly intermestic nature of this threat typology it is necessary, when reviewing the actions of states in securitizing cyberspace, to disaggregate the analysis into its component elements; namely, domestic level responses and international responses. It is further suggested that responses at the regional level (in this case, East Asia) to these threats should be considered as a separate level of analysis to the international realm as they represent a space with a more focused set of behavioural norms than may be found in the international realm, with its wider set of customs and standards. For these reasons the following section will be divided into three sections: (1) Domestic responses, (2) Regional responses, and (3) International responses.

Responses (I): Domestic

Across the East Asian region different countries face different challenges in securing cyberspace. For some, such as Japan or South Korea, connections to the web are commonplace and there is a rapid adoption of new technologies that further entrench cyberspace as a critical medium of communication and information exchange. In other countries, such as Laos or Vietnam, the presence of the Internet is very restricted; as much by capacity (economic and human) as well as by design (via state policies). The differences in Internet connectivity have a direct correlation with a state's economic modernisation as well as with its integration with global processes of development. These underlying factors and the resulting cyber presence in each of these countries, in turn, have a direct effect on the types of cyber security challenges they face. Thus, in considering how regional countries seek to improve their cyber security, an understanding of these differences and their impact on the domestic responses to the securitization of cyberspace is essential.

East Asian states have wide political and social differences, which has direct implications for securitizing cyber issues. These implications can be seen as directly stemming from the different ways the state-individual relationship is cast. In the authoritarian, nationalist and feudal countries, the state is seen as a necessary mechanism to protect its society from harm, even when pluralist systems are present. However, the society and the state are conflated such that it is up to the government to decide if a particular issue constitutes a threat. In the more politically-liberal and democratic states citizens and organizations have a wider remit for the self-assessment of cyber (and other) threats; although the state still remains the main organising and securitizing institution.

Partly reflective of the different social and political systems across the region, there are also wide disparities in economic capacity and the maturity of local markets. This leads to gaps in resource allocation for the development of Internet connections and the fostering of web-centric skills among the population. Further, as countries develop

their ability to manage web-based information and respond to cyber insecurities will be tested unless the capacity gaps are bridged.

These differences shape East Asian countries approaches to cyber security issues. Most significantly they shape how each state defines a cyber threat and how that state then responds to the insecurity. The threat deemed to be posed by certain types of online materials is a case in point. The more authoritarian the regime, the more likely it is to restrict citizens access to online materials. Hence, in countries such as Vietnam, China or Myanmar online users are regularly banned from visiting websites that have content which the state has deemed inappropriate. This classification is often given to website content which challenges the dominant orthodoxy of the state.[27] In contrast, countries such as the Philippines and Thailand – both of which face a range of political, economic and social challenges – have relatively open access to web-based materials, even though Internet penetration is uneven across both states. It is worth noting that the comparatively underdeveloped nature of the more restrictive states also creates a capacity shortfall in their ability to develop effective cyber censorship regimes. In the case of China, it has created partnerships with global computer firms (such as Yahoo and Google) to prevent domestic access to international websites.[28] Intermestic approaches to securitized threats can also work against citizens in regional countries as much as they can prevent harm.[29]

Cultural norms can also override this liberal-economic understanding. Japan, for example, has been criticized for the types of pornography local ISPs host, particularly those holding photos (and other graphical material) depicting child pornography.[30] Simply because a country has a high level of economic development and a liberal-democratic political system does therefore not automatically guarantee a shared set of norms and values with other, similarly developed, countries. In the case of Japan, these websites are not always seen as constituting a threat but other countries, whose citizens access the materials, disagree. Moreover, a high level of economic and social development coupled with a high degree of Internet penetration doe not guarantee a relaxed attitude to Internet access. In the case of Singapore, a socio-economically advanced state, access to most websites is allowed but some, domestically and internationally, are still denied.[31]

Beyond state definitions as to what is allowed and what is not (and hence what does not threaten the state's interests and what does), is also the wide variety of state responses to breaches of its cyber protocols. In Myanmar or China the severity of punishment ranges from large fines or lengthy imprisonment.[32] Vietnam tends to imprison or fine those who view restricted web content – regardless of whether it is from a local or international ISP.[33] Other, more politically liberal, countries normally restrict punishment to fines or confiscation of computer equipment; although depending on the type of offence a jail term may also be enforced.[34]

Hence, in constructing an intermestic approach to cyber security in East Asia there are a range of issues stemming from political and economic development or orientation It should again be noted that these disparities also presents a challenge to the application of the securitization model, which was formed in the more homogenous political and economic environment of Europe. All of which makes developing a regional-level response to cyber insecurities in East Asia difficult, but not impossible.

Responses (II): Regional

> Regional initiatives have two main advantages because they are pursued within an environment where there are 'fewer' cultural differences and 'fewer' problems of compatibility in judicial systems and can focus on specific problems that often complement other political and economic joint efforts (economic integration, e.g. APEC). In addition to historical and geographical homogeneity and contiguity, the differences in political and economic development in a particular region may not be too dramatic as to create mutual suspicion, and even where this exists, they can be counterbalanced by other cohesive factors.[35]

Regional approaches to security threats are not new. Since the founding of the ASEAN Regional Forum in 1994, East Asian states and their extra-regional dialogue partners have discussed ways to alleviate regional insecurities. In the post 9/11 environment, other regional organizations – such as APEC – have also moved to include regional security issues on their policy agendas. In this sense, cyber security threats have benefited from pre-existing as well as recently introduced regional security mechanisms. Thus, even as states seek to overcome shortfalls in cyber capacity, they are working within regional organizations such as the ASEAN-related institutions and APEC, to mitigate the challenges posed by cyber security threats.

In ASEAN attempts to secure cyberspace have come in two forms. First, there has been a generalized attempt to improve regional capacity and resources through the e-ASEAN process. Second, there has been a set of more explicit attempts to secure cyberspace from transnational subversion of national security; especially those stemming from the activities of criminal and terrorist organizations. APEC has taken a different approach, with cyber issues being mainly dealt with under the telecommunications area; although, as with ASEAN, more recent efforts have focused have explored ways to combat transnational crime and terrorism. For both organizations the need to address the cyber security threats perceived to stem from criminal and terrorist groups is currently the main focus of regional attention, although the cyber development aspect is also considered critical – if only to help address what are seen as the root causes of crime and terrorism (that spill over into the regional cyberspace), namely poverty and underdevelopment.

The e-ASEAN Initiative began in 1999 at the Manila Summit with the aim of developing "a broad-based and comprehensive action plan including physical, legal, logistical, social and economic infrastructure needed to promote an ASEAN e-space, as part of an ASEAN positioning and branding strategy."[36] The principle aim of this Initiative was to collectively explore methods by which the lesser-developed Southeast Asian states could overcome the digital divide with other ASEAN states by providing opportunities for them to improve their socio-economic standing through the utilisation of information and communication technologies; creating with Singapore Prime Minister Goh described as "a single electronic space".[37] The goal of this Initiative was thus to use e-strategies to foster deeper integration within ASEAN. This Initiative led to the signing of the e-ASEAN Framework Agreement in 2000, which has – in turn – become a platform for deeper regional cooperation, especially in the fields of ICT and e-commerce.[38]

Since the Framework Agreement was signed in 2000, ASEAN cooperation in this area has deepened and expanded. The Singapore declaration was adopted by the ASEAN Telecommunications and IT Ministers (TELMIN) in September 2003. This declaration (as well as the outcomes from the 2002 Manila TELMIN meeting) has led to a number of states signing Multilateral and Bilateral Mutual Recognition Agreements (MRAs). A network of ICT training centres has been established in the region to assist small and medium sized enterprises; in addition to a number of joint policy projects designed to enhance regional regulatory development in a more coordinated manner.[39] Inasmuch as ASEAN has sought to deepen regional cyber linkages and capacity it has also engaged China (under ASEAN+1 auspices) in the formation of new ICT networks for technology and application development, human resource advancement and the construction of secure networks able to resist exploitation by regional and international cyber criminal organizations.[40] Japan and South Korea have also become involved in this process under the ASEAN+3 mechanism.

With these programs acting as a catalyst for closer cooperation on cyber issues, ASEAN has begun to address the more "traditional" cyber security issues of transnational cyber crime and cyber terrorism. In some processes, such as the TELMIN meetings, cyber security issues are linked with e-development programs. For example, as a part of this process, ASEAN countries have been developing National Computer Emergency Response Teams (CERTs), with the goal of having all ten member states operationalize CERTs by 2005. The TELMINs are also overseeing the creation of "a virtual forum for ASEAN cybersecurity [*sic*]…to develop a common framework to coordinate exchange of information, establishment of standards and cooperation among enforcement agencies."[41]

By mid 2001, ASEAN's attention had turned to dealing with the regional aspects of cyber crime.[42] This was followed up by a commitment from the ASEAN Ministers responsible for transnational crime to strengthen cooperation against cyber crime given its "serious impact on the peace, security, prosperity and progress of ASEAN and on its social and moral fabric."[43] Post 9/11 cyber security issues were still pursued by ASEAN but, in many respects, had been conflated with regional and global anti-terrorism efforts. To a certain extent 9/11 provided a boost to efforts to securitize cyber security at the regional level. However, although the speech acts by regional leaders and senior officials and their related documents used securitizing language, the efforts were political – with studies of regional countries legal systems, information exchanges, and attempts to develop extradition treaties among the main responses.[44] Further, given the relative newness of cyber terrorism as an identified threat to ASEAN, such measures were comparatively mild. Since 2003, greater attention has been paid to developing responses to cyber security threats in a more "robust and coordinated manner."[45] In 2004, the members of the ASEAN Regional Forum endorsed the establishment of a regional mechanism to combat cyber terrorism. How this is to be operationalized is yet to be clarified; nonetheless it does represent a further entrenchment of cyber security practices at the ASEAN level.

APEC, as an institution with a far broader membership base, has faced similar but different challenges in protecting its members against cyber threats. This is not overly surprising. As an economically-focused institution APEC's responses to cyber issues and threats have focused on issues such as e-commerce, identity theft,[46] and related developments, before shifting in the late 1990s to focus on the criminal aspects of

cyberspace (particularly information security), and then post 9/11 to focus on cyber terrorism. Further, there is a far greater digital divide between APEC members than that which exists between ASEAN members.

Since the turn of the century, APEC has been directing an increasing array of resources to combating regional criminal and terrorist cyber threats. This shift was reflected in the decision to change "the name of the Electronic Authentication Task Group to the eSecurity Task Group and to extend its role to include information and communication technology security and information infrastructure protection."[47] Following 9/11, a succession of APEC meetings between 2001 and 2003 concentrated on the protection of critical infrastructures (especially information and communications).[48] This culminated (for the purposes of this paper) in the adoption of the *Cybersecurity Strategy* by the APEC leadership in 2003.[49] This document contained a number of recommendations including the adoption by member states of legal instruments to enforce cyber security. From an intermestic perspective this was a significant recommendation as APEC directed that the legal systems be consistent with both relevant United Nations resolutions but also the Convention on Cybercrime. In other words, to tackle the threat posed by cyber insecurities in Asia was seen to require domestic and regional responses in conjunction with international efforts; an integrated three-tier program.

Within the Cybersecurity Strategy document, APEC (overlapping with ASEAN) also argued for the creation of CERTs in its member countries. Given the wide membership of APEC, with a significant number of members involved in other regional organizations (such as Mercosur and Caricom), this program can be considered inter-regional in scope. Furthermore, as these other organizations are still predominantly state-centric, the APEC CERT program created a space for an intermestic approach to cyber security be taken inter-regionally; effectively binding APEC cyberspace pan-regionally. In terms of addressing cyber threats this organisational linkage between the APEC member economies is more effective than the ASEAN-only approach. Moreover, with APEC membership based on economies the APEC CERTS included Taiwan and Hong Kong – two of the most networked economies in the region. A failure of the ASEAN and ASEAN+ approaches is that these two localities are not included in the regional cyber security discussions, thereby creating potential gaps to exist in the regional cyber security architecture.

APEC has also begun to study ways to develop a cyber crime investigation agency between its member economies.[50] This is a good example of the benefits of an intermestic approach in addressing security threats. At one level this will be based on members jurisdictions; however, at another level, it will be a regional mechanism able to coordinate responses between APEC's 21 members. Another example of the utility of an intermestic approach to cyber security can be seen in the January 2003 decision by APEC to work with the OECD in developing guidelines to enhance cyber security.[51] This has since been followed with further meetings between the OECD and APEC, including a Malware workshop in April 2007. This was immediately proceeded by a joint APEC-ASEAN workshop on Network Security, allowing both sets of participants to interact and share knowledge and practices.[52] Importantly, APEC – far more so than ASEAN – is proactive in engaging with the business sector and, more recently, civil society organizations, in ensuring that its activities have the widest possible input and support.

However, the challenge in combating cyber insecurities lies not just at the regional level but also at the wider international level. It is therefore essential that any intermestic analysis of cyber security also include this tier.

Responses (III): International

> As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all.[53]

For the purposes of this paper, the international level is broadly defined as those activities by major states or key organizations that take place outside of the East Asian region. The role played by the United Nations in developing global responses to combating cyber threats is important to any study of cyber security. The European Union has developed one of the most comprehensive cyber security agreements of any transnational organisation and should also be studied. Each of these international actors will now be discussed in turn.

The United Nations only began to turn its attention to cyber security in the late 1990s. During the 53rd Session of the General Assembly (GA) in 1998 – after two years of meetings between member states – it promulgated Resolution 53/70; essentially a starting point for discussions on the impact of information and telecommunications technology on international security.[54] One of the key issues raised in this early resolution was the necessity of combating "information terrorism and criminality."[55] From this beginning the United Nations has moved into focusing its efforts more comprehensively on cyber security.

During its 58th session in 2003 the United Nations GA passed resolution 58/199, which sought to outline a basic framework for the creation of a global cyber security regime through the protection of critical infrastructure.[56] This built on earlier resolutions regarding the establishment of a basic framework for the creation of a global cyber security culture (GA 57/239) and the need to combat the criminal misuse of information technology (GA 56/121).[57] The key thrust of GA 58/199 was that "effective protection requires communication and cooperation nationally and internationally among all stakeholders and that national efforts should be supported by effective, substantive international and regional cooperation among stakeholders."[58] In keeping with its mandate, the United Nations was active in discussing the resolutions not only with states but also with a wide range of private sector corporations as well as domestic and international civil society organizations.

The effect of these resolutions has been to create a policy umbrella under which regional and state responses to the securitization of cyberspace can emerge. This effect highlights the crucial importance of the international aspect to intermestic cyber policies and programs; namely the need to not only work transnationally to mitigate the threat level posed by cyber insecurities (especially in terms of capacity building and knowledge exchange) but also to use transnational policy regimes to shape the development of member states domestic policies. For cyber threats it can be argued that effective securitization not only lies in the deployment of effective resources to alleviate the threat but also requires states to ensure that their legislative responses are harmonized with other states. Indeed, when examining the securitization of threats at the intermestic level,

this process of conformity could represent a third stage of the process. Without such harmonization it would be difficult to ensure transnational cooperation in a correct assessment of a cyber threat, in the resolution of the cyber threat, and in the punishment of those responsible for launching the threat.

Harmonization does not, however, only come from above. Other, sub-global, organizations or institutions can also provide effective leadership in addressing the multitude of threats that may emanate from cyberspace. The work of the European Union in this area is one such example.

At a similar point in time to the United Nations, the European Union began to formally consider the destabilising impact cyber threats could have on its member states, their markets and societies. In 1997 an expert committee on crime in cyberspace was established by the Council of Ministers "to prepare a 'legally binding instrument', which in Council of Europe terms, means an international treaty."[59] Prior to this the Council of Europe (CoE) had been considering the effects of cyber security, particularly criminal offences. These earlier efforts were kick-started in 1989 when the European Committee on Crime Problems issued a report recommending member states develop criminal legislation in respect to certain actions undertaken via a computer network (for example, hacking).[60] This was followed up in 1995, when the CoE issued a report that further reviewed the progress by member states in developing criminal law connected with information technology.[61] The conclusion of the background study to the report noted that implementation of the recommended legislation by members states had been haphazard, with some members not implementing anything and other only implementing certain aspects. It was the threat perceived to flow from cyberspace as well as from the uneven and incomplete legislative development that triggered the formation of the expert committee to prepare binding legislation at the European – as opposed to national – level.

The end result, the 2001 European Convention on Cyber-Crime (also referred to as the Budapest Convention), is considered a landmark treaty addressing cyber security matters at the domestic and regional level. Moreover, the inclusion of Canada, Japan, South Africa and the United States in the drafting process meant that the Convention has a reach beyond the boundaries of Europe. From an intermestic perspective the key section of the Convention is that which deals with harmonization of legislation and the transnational reach of law and order officials in pursuing cyber crimes across borders. As Csonka noted, although the harmonization aspect did cause some concern with the European states and the four drafting partners, the Convention still gained sufficient support to enter into force within 18 months.[62]

By mid 2004, the signatories to the Convention had expanded to 37 states.[63] In terms of transnational cooperation, the Convention requires ratifying states to provide the broadest cooperation possible. The Convention also goes further than the CERT idea, with ratifying states committed to providing national contact points for cyber offences "24/7"; in other words, 24 hours a day, 7 days a week. The 24/7 network personnel – based on pre-existing (but more limited) G8 network – not only provides technical assistance but may also directly participate in the investigation, albeit within the limits of the Convention.[64] In creating this binding instrument the CoE and the drafting partners all sought the inclusion of the private sector as well as civil society organizations. While several groups had reservations regarding privacy and individual freedom issues, the

Convention's rapid adoption – in a political region where civil rights are considered paramount – is also a signal of widespread acceptance.

Indeed, so widespread has the convention been accepted that what began as a regional initiative is now becoming a global standard, both for cooperation as well as best practice. In April 2007, for example, the Council of Europe (CoE) presented the Convention to a joint APEC/ASEAN meeting on cybercrime, which led to cooperation between the CoE and the Philippines as well as a later request for accession from that state.[65] Indonesia has also begun to review and revise its cybercrime legislation since the April meeting.[66] In November 2007, the CoE made a similar presentation in the Gulf, which led to the *Cairo Declaration Against Cybercrime* being promulgated, information-sharing between the Gulf States and the CoE as well as new legislated initiatives against cybercrime being made in that region.[67]

Thus, at the international level, the United Nations and the European Union both provide examples of transnational policy responses that seek political solutions to perceived security challenges. While the speech acts securitizing the threats from cyberspace may be present, what has taken place so far does not seem representative of emergency modes of governance; rather collections of states – with inputs from the business sector and civil society – have deliberated over an extended period of time to address current and future cyber threats. The question that then arises is what has been the impact of these transnational policy responses? How have states – especially in East Asia – applied the lessons gained from their attempts to secure cyberspace, and what have been the outcomes?

Intermestic Approaches to Combating Cyber Insecurities: Lessons Learned

> Because everything from banks to phone systems to air traffic control to our military relies so heavily on networked computers, few individuals and institutions are impervious to this new and threatening criminal activity [transnational and domestic cyber threats].[68]

Regardless of the securitizing actor the state occupies the central role in mobilising and/or coordinating responses to the threat. The role played by the state in responding to cyber threats is therefore central in alleviating insecurities. When such threats emerge and are contained within the jurisdiction of a single territory, then the state undertakes its traditional role in safeguarding the wellbeing of its citizens – either within civil society or within the activities of its local markets. However, threats from cyberspace are crossing multiple national jurisdictions with increasing frequency. This places a new burden on the state; one that the Westphalian system leaves it ill-equipped to shoulder.[69]

To address cyber threats in a comprehensive manner states must cooperate with other states to achieve mutually beneficial outcomes. This requires a diminishment of sovereignty as states need to collaboration in the development of similar legislative tools. Such collaboration implies a degree of policy constraint that goes against the Westphalian ideal of absolute state sovereignty. Below the meta-level of the state, different aspects of the bureaucracy also need to work together with their counterparts in other jurisdictions to achieve success in the prevention and alleviation of cyber insecurities. Nonetheless, given the threats that can cross over from cyberspace to the real world or that can take

challenge real-world interests in their conterminous cyber territories, to adequately secure cyberspace will require a degree of sovereign sacrifice. It is worth noting that the European Convention on Cyber-Crime represents the most advanced form of sacrifice in this sector, but even in developing that Convention participating states chose not to include a provision allowing for cross-border searches because of sovereignty concerns.[70] Thus, even the most advanced legal instrument for the intermestic alleviation of cyber insecurities faces sovereign limitations.

However, the actions of the state – even in terms of mobilising and/or coordinating responses to cyber insecurities – may prove insufficient when dealing with threats that do not engage with state interests in real-time. What is required to overcome this deficiency is a higher degree of collaboration between the public sector and the private sector. As Ortis and Evans note, "The state-firm relationship is perhaps the most important dyad for the overall growth and development of the Internet in the Asia-Pacific region."[71] The challenge in developing this partnership to secure cyberspace is to enhance overall cyber security without threatening the security of individuals or groups who use the web for legitimate purposes. One example of a successful public-private initiative to secure cyberspace can be seen in the United States National Infrastructure Protection Centre "in the coordination of training for cyber investigations and infrastructure protection in government and the private sector."[72]

Generally such partnerships are seen in domestic settings, but as globalisation and regionalisation, have become dominant forces in geo-politics, multinational corporations have expanded this partnership to include extra-national relationships with other governments. This is another aspect of the intermestic model often overlooked. One example of this was seen in March 2004 when four US-based companies – America Online, Earthlink, Microsoft and Yahoo – filed joint lawsuits against over 100 potential spam operators, whose operations were not limited to the United States.[73] Conversely, national governments are also targeting the operations of those companies whose activities on foreign ISPs contravene state legislation.[74] These actions have, in turn, prompted governments in Asia to consider how best to protect their cyber systems. These examples also highlight the duality of internet users. Inasmuch as companies can work together with governments to secure computer systems from such intrusions, they can also be responsible for generating the problem in the first place. Hence, corporations can be both mitigators of threats as well as their genesis. The same rule also applies for states, civil society and individuals; within a state as well as transnationally.

Beyond the public and private sector it is also important to consider the role of civil society – organizations as well as individuals. The involvement of civil society is essential to secure cyberspace. However, this is far more common in pluralist societies than in the more illiberal polities that characterize the East Asia region. This is a shortcoming within the ASEAN region that is only partly alleviated by the activities of APEC. Yet, as the European Convention on Cyber-Crime demonstrated, the inclusion of experts in the drafting process and the critical feedback provided by civil society organizations strengthened the final result. It should also be borne in mind that the individuals and groups that propagate viruses are also part of civil society. Thus, the inclusion of civil society representatives is not only a key element in the positive sense of securing cyberspace but they also play a key role in generating cyber insecurities as well. As such, strategies to improve cyber security need to take into account the nature of civil

society and seek to incorporate the beneficial aspects without harming individual liberties or providing new avenues for insecurity.

Conclusion

Cyberspace is the critical medium through which most of the world operates. As technologies improve the utilisation of cyberspace is only likely to increase. However, this usage is not without cost. Increased connectivity has meant an increased openness to a new generation of threats hitherto unexperienced by states or their attendant markets and societies. These threats have only increased in magnitude as the web has expanded. These new threats require new types of responses; ones that can be enacted in both the real and virtual worlds. Meeting the challenge of ensuring cyber security across domains can therefore be seen as one of the most important issues facing the global community.

From the examination of the securitization model – both in general and against the case study of cyber security – it can be said that the model has a number of significant limitations. First, the notion that the speech act by a securitizing actor to a target audience represents *ipso facto* an act of securitization is too limited. If the model is not expanded to include the policy response and the deployment of resources, then it is not possible to state when a particular speech act is representative of a first stage of securitization or a particularly effective rhetorical work. Second, from the case study of cyber security, it is not possible to remain within the polity-limited framework propounded by the Copenhagen School. It is essential that a transnational or intermestic analytical layer be mapped over the polity-centric notions of Buzan and Wæver. Third, when states address the challenges presented by cyber threats it is necessary for them to take into account the actions of other states as well as organizations operating in the international arena. In doing so, in taking into account what has been done successfully before by others, and in developing responses to new or existing cyber insecurities, it is optimum for states to therefore harmonize their endeavours with other states or organizations. Such policy harmonization may, in the case of cyber threats, represent a hitherto unexplored third stage of the securitization process.

In considering how best to these transnational threats states, as the main organisational unit in formulating a securitization response, need to consider what emphasis the policy approach should have – is a regional approach suitable or is a global response better situated for meeting their needs. The link between the domestic realm and the global arena is that of a vertical relationship, with the state choosing to participate in international organizations to further its own needs. However, as has been seen in other sectors (for example, the problems over economic cooperation in the WTO and GATT) the international level may not be the best place for the development of collective responses to individual states' needs. Within the international arena there are simply too many states, with too great a capacity gap, to allow for the swift resolution of a particular problem. The rapidity of change in cyberspace – and the attendant emergence of web-based threats against states, markets, societies and individuals – requires prompt action by securitizing actors if the essential medium through which most of the world's population now communicates is to be preserved.

What is needed is a supporting horizontal structure where states at similar levels of development, with similar needs can work together in enhancing their cyber security.

It is suggested that the creation of regional levels of governance has created a collaborative space whereby such horizontal activities can take place. In intermestic terms, regional programs to secure cyberspace are located at the nexus between the international and the domestic. These programs therefore allow states to develop transnational responses to cyber threats with mutual confidence in their other partners based on their similarities rather than differences. In the East Asian region, this confidence has been enhanced by the presence of regional organizations such as ASEAN, ASEAN+3, and APEC. Thus, even as problems arise in the formation of common responses to cyber threats, the other regional processes provide sufficient momentum to keep the overall response to cyber insecurities moving forward.

While this analysis may lead to the conclusion that a regional-level response (when available) to cyber security threats is the optimum choice for East Asian states, the critical role played by the United Nations and other international bodies (such as the European Union) needs to also be considered. Indeed, as shown in the regional and international response sections, transnational organizations can act as an additional securitizing (or, at least, politicizing) force in the absence of state activity. The challenge of the securitizing actor is two-fold. First, it must find and adopt an appropriate balance between regional and international approaches. Second, where the state is a member of a regional organisation, it needs to ensure that regional approaches and international norms do not diverge but instead develop in parallel. Thus, while issues of shared cultures, histories and geography may play a key role in further regional-level development of cyber security policies, the commonalities should never become the basis for differences with wider international efforts. If that were to happen the security of cyberspace would be seriously compromised, to the detriment of all who use it.

Bibliography

Ahmad, Rene. "Mahathir urges ASEAN to fight cybercrime", *The Straits Times*. 14 July 2001.

"Article X", *Computer Science Development Law*. State Law and Order Restoration Council Law 10/96, http://www.myanmar.com/gov/laws/computerlaw.html. 20 September 1996.

"ASEAN IT Managers pledge to enhance cyber security", *Xinhua*. 19 September 2003.

"ASEAN mulls Cyber Court, Cyber Law Institute", *Agence France Presse*. 27 October 1997.

"ASEAN to confront cyber, bio terrorism threats", *Japan Economic Newswire*. 21 May 2002.

"Asian countries join US-led coalition against spam", *Channel News Asia*. 16 March 2004.

Brenner, Susan. 'Cybercrime jurisdiction', *Crime, Law and Social Change*. (Vol. 46 Nos 4-5, 2006), pp. 189–206.

Broadhurst, Rod. 'Developments in the Global Law Enforcement of Cyber-crime', *Policing: An International Journal of Police Strategies & Management*. (Vol. 29 No. 3, 2006), pp. 408-433.

Buzan, Barry, Wæver, Ole and de Wilde, Jaap. *Security: A New Framework For Analysis*. (Boulder: Lynne Rienner, 1998).

Buzan, Barry and Wæver, Ole. *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press, 2003.

Cairo Declaration Against Cybercrime. Cairo, 27 November 2007. <http://www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_EN.pdf>. Accessed 17 March 2008.

Chester, Rodney. "Crooks tipped to ride cyber crime wave", *The Courier Mail*. 2 November 1999.

"Clarifying the cyber-crime fight", *The Japan Times*. 26 August 2004.

Clinton, William. *The Struggle for the 21st Century*. (London: 2001 Dimbleby Lecture, 14 December 2001).

CoE Recommendation No. R (89) 9 of the Committee of Ministers to Member States. Adopted 13 September 1989.

CoE Recommendation No. R (95) 13 of the Committee of Ministers to Member States. Adopted 11 September 1995.

Council of Europe. 'Project on Cybercrime: Progress Report', 30 November 2007. <http://www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/cy%20Project/567-d-2progrep2%20Final1%20pub12%20dec%2007_en.pdf>. Accessed 17 March 2008.

Csonka, Peter. "The Council of Europe Convention on Cyber Crime: A Response to the Challenge of the New Age", in Broadhurst, Roderic and Grabosky, Peter (eds.) *Cyber Crime: The Challenge in Asia*. (Hong Kong; Hong Kong University Press, 2005), pp. 303-326.

"Cyber crime rate increases 500 fold in 5 years", *The Korea Times*. 9 June 2003.

'Cybercrime report from Japan', 2 March 2006. <http://www.crime-research.org/news/02.03.2006/ 1856/>. Accessed 17 March 2008.

Deva, Surya. 'Corporate Complicity in Internet censorship in China: Who Cares For the Global Compact or the Global Online Freedom Act?', *The George Washington International Law Review*. (Vol. 39 No. 2, 2007), pp. 255-319.

Drennan, Peter. "Enforcement and the Public Private Sector Interface", in Broadhurst, Roderick (ed.). *Proceedings of the Asia Cyber Crime Summit, Hong Kong 2001*. (Hong Kong; Centre for Criminology, 2001). pp. 204-207

e-ASEAN Framework Agreement. Singapore. Signed 24 November 2000.

"Europe looks to fight cyber-crime", *The South China Morning Post*. 16 September 2004.

"Going by the back door to view banned sites", *The Straits Times*. 1 May 2000.

Government of the United States of America. *National Strategy to Secure Cyberspace*. Washington, February 2003.

<http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html>. Accessed 17 March 2008.

Huang, Xiaomin, Peter Radkowski III and Peter Roman. 'Computer Crimes', *The American Criminal Law Review*. (Vol. 44 No. 2, Spring 2007), pp. 286-335.

"ICT & E-Commerce", *http://www.aseansec.org/6269.htm*. [20 April 2005].

"Internet Begins 30 Years Ago at UCLA", http://www.engineer.ucla.edu/stories/netis30.htm. Accessed 6 April 2005.

"IIT Firewall Against Pak Hacker Threat", *The Statesman (India)*. 15 August 2003.

Jacob, Paul. "E-ASEAN: 10 states, one cyber region", *The Straits Times*. 26 November 1999.

"Japanese government sites targeted for cyber attacks", *Deutsche Press-Agentur*. 14 April 2005.

Jesdanun, Anick. "Study Finds Chinese filters sophisticated", *The Associated Press*. 14 April 2005.

Joint Communiqué of the Third ASEAN Ministerial Meeting on Transnational Crime (AMMTC). Singapore: 11 October 2001.

Kakuchi, Suvendrini. "Japan: Tougher Action Sought on Child Pornography on the Web", *Inter Press Service*. 15 June 2000.

Kegley, Charles and Wittkopf, Eugene. *World Politics: Trends and Transformation*. (New York: St Martins Press, 1981).

Korean National Police Agency. *Cyber crime statistics (by type)*, <http://www.police.go.kr/KNPA/statistics/st_investingation_02.jsp>. Accessed 17 March 2008.

Liedtke, Michael. "Googles Chinese News Service Omits government-banned sites", *The Associated Press*. 24 September 2004.

Mayall, James. "Non-intervention, Self-determination and the 'New World Order'", *International Affairs*. (Vol. 67 No. 3, July 1991) pp. 421-429.

McCusker, Rob. 'Transnational organised cyber crime: distinguishing threat from reality', *Crime, Law and Social Change*. (Vol. 46 Nos 4-5, 2006), pp. 257–273.

Memorandum of Understanding Between The Association of Southeast Asian Nations and the People's Republic of China On Cooperation in Information and Communications Technology. (Indonesia, Bali: signed 8 October 2003).

"No. of cyber-crimes surpassed 2,000 last year", *Japan Economic Newswire*. 24 February 2005.

"NPA, SDF websites hit by cyber attacks", *The Daily Yomiuri (Tokyo)*. 15 April 2005.

Orlowski, Steve. "APEC Activities to Address Cyber-crime through Public-Private Sector Cooperation", in Broadhurst, Roderick (ed.). *Proceedings of the Second Asia Cyber Crime Summit, Hong Kong 2003*. Hong Kong; Centre for Criminology, 2003. pp. 37-45.

Ortis, Cameron and Evans, Paul. "The Internet and Asia-Pacific Security: old conflicts and new behaviour", *The Pacific Review*. (Vol 16 No.4, 2003) pp. 549-570.

"Pakistan Official Confirms Indian Hacker Attack on Internet Service", *BBC Monitoring International Reports*. 27 March 2005.

Pollitt, Michael. "The Online Mafia: Cyber Gangsters Are Using Computer Networks to Blackmail Businesses", *The Independent*. 15 December, 2004.

Recommendation by the APEC Telecommunications and Information Working Group (TEL) to APEC Senior Officials (SOM) For An APEC Cybersecurity Strategy. August 2002.

Review of Cybercrime Legislation in Indonesia, <http://www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/default_en.asp>. Accessed 17 March 2008.

Risse-Kappen, Thomas (ed.). *Bringing Transnational Relations Back In: Non-State Actors, Domestic Structures and International Institutions*. (Cambridge, Cambridge University Press, 1995).

"RSF Urges release of cyber dissident", *BBC Monitoring International Reports*. 6 August 2002.

Shannon, Julie and Thomas, Nick. "Human Security and Cyber Security: Operationalising a Policy Framework", in Broadhurst, Roderic and Grabosky, Peter (eds.) *Cyber Crime: The Challenge in Asia*. (Hong Kong; Hong Kong University Press, 2005), pp. 327-346.

Shehu, Abdullahi Y. "International Cooperation in Combating Cyber-crime: a Public/Private Sector Coalition in Asia", in Broadhurst, Roderick (ed.). *Proceedings of the Asia Cyber Crime Summit, Hong Kong 2001*. (Hong Kong; Centre for Criminology, 2001). pp 117-133.

"Specialists see change in cyber crimes", *The Canberra Times*. 1 April 2005.

Sussmann, Michael. "The Critical Challenges From International High-Tech and Computer-Related Crime at the Millennium", *Duke Journal of Comparative and International Law*. (Vol. 9, 1999). pp. 451-489.

Symantec. *Symantec Internet Security Threat Report: Trends for January-June 2007*. September 2007, <http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf>. Accessed 17 March 2008.

TEL Chair. *Cyber Crime/Cyber Security Activities Report APEC TEL Working Group*. Counter-Terrorism Task Force Meeting. Khon Kaen, Thailand. 26 May 2003.

Thomas, Daniel. "National Hi-Tech Crime Unit smashes online extortion racket", *Computing*. 21 July 2004.

Nicholas Thomas and Curley, Melissa, 'Advancing East Asian Regionalism: An Introduction', in Curley, Melissa and Thomas, Nicholas (eds). *Advancing East Asian Regionalism*. (London: RoutledgeCurzon, 2007). pp. 1-25.

Thomas, Nick. "Building an East Asian Community: Origins, Structure and Limits", *Asian Perspectives*, Vol. 26, No. 4 (Seoul: Kyungnam University, 2002), pp. 83-112.

"Toward an e-ASEAN", http://www.aseansec.org/6268.htm. [20 April 2005].

United Nations General Assembly Resolution 53/70 *Developments in the Field of Information and Telecommunications in the context of International Security*. 4 December 1998.

United Nations General Assembly Resolution 56/121 *Combating the Misuse of Information Technologies*. 19 December 2001.

United Nations General Assembly Resolution 57/239 *Creation of A Global Culture of Cyber Security*. 20 December 2002.

United Nations General Assembly Resolution 58/199 *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*. 23 December 2003.

Urbas, Gregor. "Cyber-crime legislation in the Asia-Pacific Region", in Broadhurst, Roderick (ed.). *Proceedings of the Second Asia Cyber Crime Summit, Hong Kong 2003*. (Hong Kong; Centre for Criminology, 2003). pp. 94-122.

"Vietnam, APEC Fight Cyber Criminals", *Vietnam News Briefs*. 27 August 2004.

"Vietnam: UN Delegates should condemn Internet Arrests", *http://hrw.org/press/2003/03/vietnam033103.htm*. 31 March 2003. [23 April 2005].

Wæver, Ole. "On Securitization and Desecuritization", in Lipshutz, Ronnie (ed.). *On Security*. New York: Columbia University Press, 1995. pp 46-86

"What's clicking in Singapore – fear and censoring on the e-campaign trail", *The Associated Press*. 15 July 2001.

"Yahoo 'complicit' in China rights abuses through censorship pledge: group", *Agence France Presse*. 9 August 2002.

[1] "Clarifying the cyber-crime fight", *The Japan Times*. 26 August 2004.

[2] Comments by Ulrich Sieber, Head, Max Planck Institute for Foreign and Criminal Law. See "Europe looks to fight cyber-crime", *The South China Morning Post*. 16 September 2004.

[3] Henry Kissinger, as quoted in Kegley, Charles and Wittkopf, Eugene. *World Politics: Trends and Transformation*. (New York: St Martins Press, 1981) p. 29.

[4] For more on recent community-building efforts in East Asia by the author see: Nicholas Thomas and Curley, Melissa, 'Advancing East Asian Regionalism: An Introduction', in Curley, Melissa and Thomas, Nicholas (eds). *Advancing East Asian Regionalism*. (London: RoutledgeCurzon, 2007), pp. 1-25; and Thomas, Nick. "Building an East Asian Community: Origins, Structure and Limits", *Asian Perspectives*, Vol. 26, No. 4 (Seoul: Kyungnam University, 2002), pp. 83-112.

[5] For the purposes of this paper the analysis at the domestic level will be focused only on the thirteen countries involved in the ASEAN+3 process (Japan, South Korea, China, Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Singapore, Thailand, the Philippines and Vietnam). This limitation has been chosen as it allows for analysis to be undertaken at the domestic, regional and international levels. Hence,

North Korea and Mongolia will not be used as examples. Taiwan and Hong Kong – while, in regional terms, part of China – will also not be relied upon.

[6] "No. of cyber-crimes surpassed 2,000 last year", *Japan Economic Newswire*. 24 February 2005.

[7] See: 'Cybercrime report from Japan', 2 March 2006. <http://www.crime-research.org/news/02.03.2006/1856/>. Accessed 17 March 2008.

[8] "Cyber crime rate increases 500 fold in 5 years", *The Korea Times*. 9 June 2003.

[9] See: Korean National Police Agency. *Cyber crime statistics (by type)*, <http://www.police.go.kr/KNPA/statistics/st_investingation_02.jsp>. Accessed 17 March 2008.

[10] See comments by Greg Stone, as quoted in: "Specialists see change in cyber crimes", *The Canberra Times*. 1 April 2005.

[11] For both sets of data see: Symantec. *Symantec Internet Security Threat Report: Trends for January-June 2007*. September 2007, <http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf>. Accessed 28 February 2008.

[12] As Broadhurst has noted the total number of users in China is expected to 'exceed the number in North America by 2008'. See: Broadhurst, Rod. 'Developments in the Global Law Enforcement of Cyber-crime', *Policing: An International Journal of Police Strategies & Management.* (Vol. 29 No. 3, 2006), pp. 408-433. [quote on p. 411]

[13] Over the September Labour Day weekend in 1969 the first computer at UCLA was hooked up to APRANET, the forerunner what became known as the Internet during the 1980s. See: "Internet Begins 30 Years Ago at UCLA", http://www.engineer.ucla.edu/ stories/netis30.htm. Accessed 6 April 2005.

[14] Mayall, James. "Non-intervention, Self-determination and the 'New World Order'", *International Affairs*. (Vol. 67 No. 3, July 1991) pp. 421-429.

[15] Risse-Kappen, Thomas (ed.). *Bringing Transnational Relations Back In: Non-State Actors, Domestic Structures and International Institutions*. (Cambridge, Cambridge University Press, 1995). p. xi

[16] Consider that in 1993 there were only 50 websites, mostly based in the United States. By the turn of the century there were over 350 million registered sites around the world. See: Clinton, William. *The Struggle for the 21st Century*. (London: 2001 Dimbleby Lecture, 14 December 2001).

[17] Buzan, Barry, Wæver, Ole and de Wilde, Jaap. *Security: A New Framework For Analysis*. (Boulder: Lynne Rienner, 1998).

[18] Government of the United States of America. *National Strategy to Secure Cyberspace*. Washington, February 2003. p 6

[19] For more on desecuritization see: Ole Wæver. "On Securitization and Desecuritization", in Ronnie Lipshutz (ed.). *On Security*. New York: Columbia University Press, 1995. pp 46-86.

[20] Buzan, Barry and Wæver, Ole. *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press, 2003. p 489.

[21] As the effectiveness of the resource allocation is dependent on the nature of the threat – which may be dynamic – effectiveness need not be considered as part of the extension of the securitization model.

[22] Source: "Japanese government sites targeted for cyber attacks", *Deutsche Press-Agentur*. 14 April 2005; and "NPA, SDF websites hit by cyber attacks", *The Daily Yomiuri (Tokyo)*. 15 April 2005. Similar events have also taken place between other feuding countries in Asia. See for example: Pollitt, Michael. "The Online Mafia: Cyber Gangsters Are Using Computer Networks to Blackmail Businesses", *The Independent*. 15 December, 2004, and Thomas, Daniel. "National Hi-Tech Crime Unit smashes online extortion racket", *Computing*. 21 July 2004.

[23] See, for example: "Pakistan Official Confirms Indian Hacker Attack on Internet Service", *BBC Monitoring International Reports*. 27 March 2005, and "IIT Firewall Against Pak Hacker Threat", *The Statesman (India)*. 15 August 2003.

[24] It should be noted that official documents use the terms cyber-crime and cyber security interchangeably. This paper suggests that a more critical usage would assist in the understanding of these threats by more precisely defining their characteristics.

[25] See Shannon, Julie and Thomas, Nick. "Human Security and Cyber Security: Operationalising a Policy Framework", in Broadhurst, Rod and Grabosky, Peter (eds.) *Cyber Crime: The Challenge in Asia*. (Hong Kong; Hong Kong University Press, 2005), pp. 327-346. On "Titan Rain" see for example: "The dragon plays catch-up in world of cyber spy", *The New Zealand Herald*, 7 September 2007.

[26] McCusker, Rob. 'Transnational organised cyber crime: distinguishing threat from reality', Crime, Law and Social Change. (Vol. 46 Nos 4-5, 2006), pp. 257–273.

[27] For how this is done in the case of China see: Jesdanun, Anick. "Study Finds Chinese filters sophisticated", *The Associated Press*. 14 April 2005.
[28] See: Liedtke, Michael. "Googles Chinese News Service Omits government-banned sites", *The Associated Press*. 24 September 2004, and "Yahoo 'complicit' in China rights abuses through censorship pledge: group", *Agence France Presse*. 9 August 2002.
[29] For an extension of this argument see: Deva, Surya. 'Corporate Complicity in Internet censorship in China: Who Cares For the Global Compact or the Global Online Freedom Act?', *The George Washington International Law Review*. (Vol. 39 No. 2, 2007), pp. 255-319.
[30] Kakuchi, Suvendrini. "Japan: Tougher Action Sought on Child Pornography on the Web", *Inter Press Service*. 15 June 2000.
[31] These sites usually relate to pornographic content but concerns have been raised in a recent election about censorship of online political materials via biased regulations. See: "Going by the back door to view banned sites", *The Straits Times*. 1 May 2000, "What's clicking in Singapore – fear and censoring on the e-campaign trail", *The Associated Press*. 15 July 2001.
[32] The case of Li Dawei (China) is illustrative. Li downloaded pro-democracy texts from the Web and was subsequently sentenced to 11 years imprisonment for "trying to subvert state power". Source: "RSF Urges release of cyber dissident", *BBC Monitoring International Reports*. 6 August 2002. In Myanmar even owning an unregistered modem can result in imprisonment. For further information see "Article X", *Computer Science Development Law*. State Law and Order Restoration Council Law 10/96, http://www.myanmar.com/gov/laws/computerlaw.html. 20 September 1996.
[33] For information on some of the cases in Vietnam see: "Vietnam: UN Delegates should condemn Internet Arrests", *http://hrw.org/press/2003/03/vietnam033103.htm*. 31 March 2003. Accessed 23 April 2005.
[34] A good summary of the different laws and punishments in regional countries is contained in: Urbas, Gregor. "Cyber-crime legislation in the Asia-Pacific Region", in Broadhurst, Roderick (ed.). *Proceedings of the Second Asia Cyber Crime Summit, Hong Kong 2003*. (Hong Kong; Centre for Criminology, 2003). pp. 94-122.
[35] Shehu, Abdullahi Y. "International Cooperation in Combating Cyber-crime: a Public/Private Sector Coalition in Asia", in Broadhurst, Roderick (ed.). *Proceedings of the Asia Cyber Crime Summit, Hong Kong 2001*. (Hong Kong; Centre for Criminology, 2001). p. 130.
[36] Source: "Toward an e-ASEAN", http://www.aseansec.org/6268.htm. [20 April 2005]. Interestingly, even before the e-ASEAN Initiative was proposed there were regional discussions on the need to create an ASEAN Cyber Court to regulate regional e-commerce. These were partly in reaction to the US proposal on Global Electronic Commerce (July 1997). However, the Cyber Court idea was dropped from the regional agenda by the time the e-ASEAN Initiative was unveiled. Source: "ASEAN mulls Cyber Court, Cyber Law Institute", *Agence France Presse*. 27 October 1997.
[37] Jacob, Paul. "E-ASEAN: 10 states, one cyber region", *The Straits Times*. 26 November 1999.
[38] See the *e-ASEAN Framework Agreement*. Singapore. Signed 24 November 2000.
[39] Source: "ICT & E-Commerce", *http://www.aseansec.org/6269.htm*. Accessed 20 April 2005.
[40] Source: *Memorandum of Understanding Between The Association of Southeast Asian Nations and the People's Republic of China On Cooperation in Information and Communications Technology*. (Indonesia, Bali: signed 8 October 2003).
[41] Source: "ICT & E-Commerce", *http://www.aseansec.org/6269.htm*. Accessed 20 April 2005.
[42] See, for example: Ahmad, Rene. "Mahathir urges ASEAN to fight cybercrime", *The Straits Times*. 14 July 2001.
[43] See Paragraphs 16 and 17 of the *Joint Communiqué of the Third ASEAN Ministerial Meeting on Transnational Crime (AMMTC)*. Singapore: 11 October 2001.
[44] See for example, the efforts contained in: "ASEAN to confront cyber, bio terrorism threats", *Japan Economic Newswire*. 21 May 2002.
[45] "ASEAN IT Managers pledge to enhance cyber security", *Xinhua*. 19 September 2003.
[46] See reports on the APEC Technomart III, as contained in: Chester, Rodney. "Crooks tipped to ride cyber crime wave", *The Courier Mail*. 2 November 1999.
[47] See: TEL Chair. *Cyber Crime/Cyber Security Activities Report APEC TEL Working Group*. Counter-Terrorism Task Force Meeting. Khon Kaen, Thailand. 26 May 2003, p. 1.
[48] Ibid.

[49] This strategy grew out of a series of recommendations that had been put to the APEC Senior Officials and Leaders the previous year by the APEC Telecommunications and Information Working Group. See: *Recommendation by the APEC Telecommunications and Information Working Group (TEL) to APEC Senior Officials (SOM) For An APEC Cybersecurity Strategy*. August 2002.
[50] "Vietnam, APEC Fight Cyber Criminals", *Vietnam News Briefs*. 27 August 2004.
[51] TEL Chair. *Cyber Crime/Cyber Security Activities Report APEC TEL Working Group*. p. 3. For more on APEC's efforts to secure cyberspace see: Orlowski, Steve. "APEC Activities to Address Cyber-crime through Public-Private Sector Cooperation", in Broadhurst, Roderick (ed.). *Proceedings of the Second Asia Cyber Crime Summit, Hong Kong 2003*. Hong Kong; Centre for Criminology, 2003. pp. 37-45.
[52] For more information see: <http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html>. Accessed 10 April 2008.
[53] From: United Nations General Assembly Resolution (hereafter GA) 57/239 *Creation of A Global Culture of Cyber Security*. 20 December 2002.
[54] See GA 53/70 Developments in the Field of Information and Telecommunications in the context of International Security. 4 December 1998.
[55] Ibid.
[56] See: GA 58/199 *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*. 23 December 2003.
[57] For more information see: GA 57/239 *Creation of A Global Culture of Cyber Security*. 20 December 2002; and GA 56/121 *Combating the Misuse of Information Technologies*. 19 December 2001; respectively.
[58] See: GA 58/199 *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*. 23 December 2003.
[59] Csonka, Peter. "The Council of Europe Convention on Cyber Crime: A Response to the Challenge of the New Age", in Broadhurst, Roderic and Grabosky, Peter (eds.) *Cyber Crime: The Challenge in Asia*. (Hong Kong; Hong Kong University Press, 2005), p 303.
[60] The outcomes of this report was strengthened by a recommendation from the Council of Europe. See: CoE Recommendation No. R (89) 9 of the Committee of Ministers to Member States. Adopted 13 September 1989.
[61] See: CoE Recommendation No. R (95) 13 of the Committee of Ministers to Member States. Adopted 11 September 1995.
[62] Csonka, Peter. "The Council of Europe Convention on Cyber Crime: A Response to the Challenge of the New Age", p 304.
[63] Ibid.
[64] Ibid. pp 324-325.
[65] See: Council of Europe. 'Project on Cybercrime: Progress Report', 30 November 2007. <http://www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/cy%20Project/567-d-2progrep2%20Final1%20pub12%20dec%2007_en.pdf >. Accessed 5 March 2008.
[66] See: *Review of Cybercrime Legislation in Indonesia*, <http://www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/default_en.asp>. Accessed 17 March 2008.
[67] See: *Cairo Declaration Against Cybercrime*. Cairo, 27 November 2007. <http://www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_EN.pdf>. Accessed 17 February 2008.
[68] Sussmann, Michael. "The Critical Challenges From International High-Tech and Computer-Related Crime at the Millennium", *Duke Journal of Comparative and International Law*. (Vol. 9, 1999). p.452. [451-489]. The section in […] was added for clarity.
[69] For a deeper discussion on this isse see: Brenner, Susan. 'Cybercrime jurisdiction', Crime, Law and Social Change. (Vol. 46 Nos 4-5, 2006), pp. 189–206.
[70] Csonka, Peter. "The Council of Europe Convention on Cyber Crime: A Response to the Challenge of the New Age", p. 326.
[71] Ortis, Cameron and Evans, Paul. "The Internet and Asia-Pacific Security: old conflicts and new behaviour", *The Pacific Review*. (Vol 16 No.4, 2003) p. 560.

[72] Drennan, Peter. "Enforcement and the Public Private Sector Interface", in Broadhurst, Roderick (ed.). *Proceedings of the Asia Cyber Crime Summit, Hong Kong 2001*. (Hong Kong; Centre for Criminology, 2001). p. 205.

[73] "Asian countries join US-led coalition against spam", *Channel News Asia*. 16 March 2004.

[74] As was the case when the French and German governments took Yahoo! to court over the sale of Nazi memorabilia from servers outside of the French/German national borders. See: Huang, Xiaomin, Peter Radkowski III and Peter Roman. 'Computer Crimes', *The American Criminal Law* Review. (Vol. 44 No. 2, Spring 2007), pp. 286-335. [quote on p.333]