KASARINLAN VOL. 17 NO 2. 2002

Is there Information Warfare in Southeast Asia?

ROLANDO TALAMPAS*

In the post-Cold War order, Southeast Asia has been one of the most volatile regions in the world. New challenges now face both state and nonstate actors. One of the most important of these is the transformation in information and communication technology and its implications for the emergence of so-called "information warfare". This paper examines the forms of information warfare in Southeast Asia, with passing reference also to Northeast Asia, in order to assess the scope of the threat and the various responses to it. It does so by locating the significance of information warfare in the context of economic development policies, the domestic politics of individual states, and the broader regional socio-cultural trajectory. The conclusion suggests that information warfare in Southeast Asia is actually on quite a modest scale but that there are important tensions emanating from Northeast Asia that may spill over into the region.

Introduction

Is Southeast Asia ablaze with information warfare? At what levels of sophistication are these countries already involved in using the information superhighway in clicking the mouse for their national interest? What conditions the involvement of some, if not all, countries in the high stakes of high-tech warfare? Taking Asia as a whole, Desmond Ball told *Far Eastern Economic Review*'s Charles Bickers, "Cyberwarfare is very buoyant in Asia right now, much more than in other parts of the world, perhaps because of the generally high levels of defence activity". He added: "Intelligence budgets around the region have more than doubled in the last few years, and much of that is electronic activity". But as he suggests, the Asian cyberwarriors have merely been "gathering intelligence and practising on their own internal systems, so that when they do press the button, it works".[1]

There is little doubt that the unstable post-Cold War environment helped to bring longstanding ethnic and other tensions within and between states to the surface.[2] The catchphrase—revolution in military affairs (RMA)—called for a rethink of the defense and security perspectives and programs. Globalization drew attention to new challenges to state and

*Author is a recipient of the Kasarinlan Writing Grant.

nonstate actors as they tread new paths out of crises and into new development trajectories.[3] Rapid transformations in information and communication technology (ICT) bolstered the use of information and knowledge, and the digital age created new binaries in an admittedly unipolar world.

Conflict has since spared no one. As Stein famously writes:

> As "first wave" wars were fought for land and "second wave" wars were fought for control over productive capacity, the emerging "third wave" wars will be fought for control of knowledge. And, since "combat form" in any society follows the "wealth-creation form" of that society, wars of the future will be increasingly "information wars".
>
> ...Conflict is about a determinate something, not an indeterminate anything. If the goal of influencing the adversary's ability to "observe" by flooding him with corrupted or contradictory information and data; disrupting his ability to "orient" by the elimination of the possibility of objective reasoning; and forcing his "decisions" to respond to a fictive or virtual universe, "actions" will, of course, be produced, but they may well be actions which are chaotic, random, nonlinear and inherently unpredictable by our side as there is no "rational" relationship of means to ends.[4]

In light of this situation, the mapping of locations and positions of adversaries in the physical battlefield has made visualizing the terrain a round-the-clock preoccupation that has increasingly relied on technology and "paradigm shift" from information to knowledge.[5] Situations of conflict are fleeting and driving that information is the weapon of choice. Information warfare has assumed a variety of forms: command and control warfare; intelligence-based warfare; economic warfare; electronic warfare; psychological warfare; hacker warfare; economic information warfare; and cyber warfare.[6]

This paper clarifies the forms of information warfare in Southeast Asia by locating the experiences of the region within the framework of economic, political and socio-cultural developments and the attendant conflicts. Despite the variety of "infowar" capabilities and potentials in the region, it is argued that cooperation may still be realized that can help prevent conflict, notwithstanding the weak intervention mechanisms currently available.

'War in the Information Spectrum'

In the period of the *Pax Americana*, information warfare is by and large a peacetime form of conflict. As such, the term information warfare has been used to connote and denote events and outcomes that involve the use of ICT. One analyst goes so far as to suggest that information warfare should be considered as "war in the information spectrum" that "targets the human mind".[7] The scope and objectives of information warfare can be characterized in the following terms:

> At the heart of information warfare (IW) is information. Information guides decisionmaking in peacetime and war at the strategic (a decision to declare war), operational (a decision to move a division of forces forward for an attack), or tactical (a decision to order an aircraft to engage) levels. These decisions in turn trigger action. The purpose of IW is to affect the adversary's decisionmaking process and associated actions to one's own advantage. The outcome for the enemy can be wrong decisions, late decisions, or no decisions at all.[8]

Manpower and other resource utilization for gaining "superiority" and/or "dominance" over a competitor or adversary has qualified the purpose of engaging in information warfare.[9] Such objectives by the practitioners and promoters of information warfare derive from the time-honored advantage quest sought in keeping the "survival value" that goes hand in hand with information. As such, information warfare has gained currency and potency as a consequence of the advent of the information age, the so-called "third wave", made real by the convergence of information and communication technologies and the preponderance of information-based industries and techniques for advancing military superiority.

Information warfare serves high end purposes in both networked and non-networked environments. The types of conflict area have thus distinguished the more restricted network centric warfare (NCW) from the general, though vague, notion of information warfare. NCW involves measures and countermeasures within the given parameters of information network technologies, while generic information warfare is taken to mean the forms such warfare assumes given certain conditions. In military usage, NCW means:

> an information superiority-enabled concept of operation that generates increased combat power by networking sensors, decision

> makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.[10]

Malice and subversive intentions of the purveyors of information operations spell out the offensive end of information warfare. Elsewhere, defense or protection also plays an important role in entertaining the use of information warfare, especially in matters pertaining to "threats" and "vulnerabilities".[11] The value and vulnerability of information make defensive objectives imperative too. The costs of defensive/protective systems far outweigh both the price of installing hightech systems and means of disabling them. This may explain why poorer countries with low-end or practically nonexistent systems spend their defense budgets elsewhere.

Southeast Asia and Information Warfare

In a recent study of the regional implications of information warfare, Ortis and Evans examine Asia Pacific internet outcomes, especially the spillover of real-life conflicts into cyberspace, with reference to the dyads formed by "states, firms, civil society and uncivil society groups".[12] In doing so, they pose a challenge to national governments to look into the risks posed by the "dark side" of the internet. Echoing their concerns, we focus on the conditions obtaining in Southeast Asia that may help us keep overstatement of the case at bay.[13] At the onset, it should be pointed out that the (un)civil society-initiated challenges have generally marked the use of information technology in engaging both states and firms in Southeast Asia. Further, there is no indication of a coming showdown in cyberspace within the civil–uncivil society divide.[14] Additionally, it is becoming apparent that the democratic content of various social movements has also informed the processes and forms of advocacy waged in both the internet and the real-life society.

The following themes cover the topic of information warfare in Southeast Asia under contemporary regional circumstances. Here, we look at three domestic aspects of the incidence of information warfare—cyber warfare—drawing out some interim conclusions: the ICT related plans and activities of most countries are related primarily to development objectives; the experiences of cyber war in the region have been directed towards

shaping domestic political events; and, the socio-cultural dynamics undergoing transformation are constrained by both the domestic and international factors.

ICT and Economic Development

The terms e-governance, e-commerce, e-learning, e-business, e-security and e-society, among others, have all been used in many official and business pronouncements of Southeast Asian countries.[15] They reflect the agendas and policy priorities of most developing and developed countries in the region. In the developing countries, ICT is framed within the need for building social capital and promoting innovation and investment.[16] However, two relatively more developed countries—Malaysia and Singapore—stand out with their long-term plans for infotech industries and related services, while the other countries lag behind in addressing the foreign investment requirements of building a robust ICT economic sector.[17] Southeast Asia is often represented and compared to the rest of the world relative to hardware and internet access (see Table 1). Relatedly, although broadband internet access (upwards of 256 Kbps) creeps in the developing world, Asia tops the world's regions in terms of percentage coverage.[18]

In 2002, five Southeast Asian countries were among the top 55 of the 150 countries in the information superhighway (see Table 2). This indication of "informatized" Southeast Asian societies may also be gleaned from the rate of economic development of the individual countries, especially in terms of historic GDP growth rates, the rates of urbanization

Table 1. **Selected IT Indicators, Sub-Regional**

Sub-Region	*Per 1,000 people (1997-2000)*	*Per 10,000 people (1998-2000)*	
	Personal Computers	*Internet Hosts*	*Internet Users*
NIEs	287	190.62	1820
China	11	0.42	88
Southeast Asia	25	7.16	227
Central Asian Republics	NA	4.56	25
Pacific	NA	0.63	3
Industrial Countries	375	1113.60	2578

Source: *World Paper ISI*, February 2002

attendant to the rise of industrial sectors and other key demographic changes. Nevertheless, there is as yet little evidence to correlate informatized societies with the battlefield transparency ends of information warfare. Despite this, cybercrime targets critical economic sectors. Malaysian, Singaporean and Thai companies, for example, were among the latest victims of intrusions in the Asia-Pacific business world.[19] With more unreported intrusion cases for fear of negative financial or reputation consequences, these three countries can easily be joined by many more.

On balance, what remains as possible domestic conflict areas are those pertaining to policies undertaken by states relevant to the promotion of ICT in bringing about progress. These policies impact on education, social services, employment, prices and the general living and working conditions of the people. In early 2002, Vietnam's Do Trung Ta, president of the Post and Telecommunications agency, put in words what might also be true of the other Southeast Asian countries' trajectory: "The State pays special attention to computerising the social and economic sectors in order to develop the IT sector to meet the demands of industrialising and modernising the country".[20]

Politics, Security and IT

An interesting facet of how reported cyberwarfare in Southeast Asia shapes the domestic political landscape is suggested by insights that reaffirm the role of the state in international politics.[21] The state is an enabling agent of the ICT revolution, via its Web presence and other information programs, which in turn is accessed to re-configure the political system.[22] However the state plays its part in the troubled parts of the region, the internet becomes its virtual battlespace where nonstate actors act out roles like mosquito squadrons:

> Across Southeast Asia, the Internet has given a potent liberation weapon to dissidents whom autocrats once simply forgot about after shunting them to dark prisons, malarial jungles, and foreign exile. Many of the dissident Internet campaigns are based abroad, so they are safe from clampdowns, yet they penetrate borders to spread news and views that the domestic media cannot touch. Internet activists, many working like journalists in a transnational newsroom, have transformed scattered voices into global dissident movements.[23]

Table 2. **Information Society Index: Selected Southeast Asian Countries (2002)**

Category	*Country*	*Rank (2000)*	*Change in 2001*	*Computer Score (Rank)*	*Internet Score (Rank)*	*Information Score (Rank)*	*Social Score (Rank)*	*Score*
Skaters	Singapore	9	4	800 (8)	2504 (2)	1953 (21)	810 (33)	6067
Sprinters	Malaysia	32	2	372 (28)	1176 (25)	1073 (36)	571 (48)	3192
Strollers	Philippines	48	3	154 (50)	326 (43)	643 (50)	781 (34)	1904
Strollers	Thailand	47	1	207 (42)	274 (46)	723 (48)	670 (39)	1874
Strollers	Indonesia	53	-1	125 (55)	122 (53)	557 (54)	488 (52)	1292

Source: *World Paper* ISI, February 2002

States bring into the picture their own forces to bear and seek to even up the score, often lending legitimacy or conferring belligerency status to the dissidents with laptop computers. IT has indeed revolutionized the political and security developments in Southeast Asia.

Burma. Burma's low economic performance has not stopped the SPDC military regime from acquiring satellite eavesdropping technology and engaging in tit-for-tat tactics against dissident National League for Democracy forces allied with Nobel Prize winner Aung San Suu-kyi. The regime's "cyber-warfare center", allegedly located at a Defence Ministry compound in Rangoon could "intercept and interfere with all sorts of telephone and fax messages as well as e-mail and radio communications". Reportedly, its "Directorate of the Defense Services Intelligence, the army junta's secret police, has launched an international campaign against opponents of the military rule by sending them computer viruses via e-mail" and propaganda campaigns via the newsgroup on soc.culture burma.[24]

Indonesia/East Timor. Indonesia and newly independent East Timor have also been the subject of long-distance sympathy cyber attacks. This involved Chinese mailbomb attacks against Indonesian Web pages in May 1998 for the alleged Indonesian government failure to "react to the alleged torture, rape, and murder of Indonesian Chinese during race riots".[25] Not to be outdone, Indonesia's "Medan Hackers" directed their attacks at Taiwan, South Korea, Japan, China and Thailand. In 2002, this reportedly cost China $865 million. According to the BBC, "Financial damage from malware such as Bugbear has caused around $2 billion in October 2002, compared to $886 million to $1.07 billion in damages caused by digital attacks".[26] Earlier, anti-Suharto cyberwarriors mounted their attacks from outside the country on at least two occasions. First, INDONESIA-L (http://www.indopubs.com/archives), maintained from Lanham, Maryland, attacked the regime from a safe distance.[27] Then, East Timor independence supporters maintained the .tp domain through the ISP named Connect-Ireland abroad.[28] Perhaps with more support, Jose Ramos-Horta also threatened to "shut down Indonesian government and banking computer systems if the country's authorities crack down on the East Timor independence movement".[29] According to Peter Eng,

> The Internet allowed Indonesians to discuss taboo subjects, such as corruption in the military and the business empires of Suharto's children, and to link up with other dissidents. It introduced new dissident groups

to a national audience. Political figures hiding from security forces spoke up on the Internet, as did journalists whose magazines had been closed by the government.[30]

If reports were true, Indonesian militants may be more capable than alleged. According to the US Department of Defense, some Indonesian-originated exemplars "studied (US) emergency telephone systems, electrical generation and transmission, water storage and distribution, nuclear power plants and gas facilities".[31]

Cambodia and Vietnam. Although these two countries lag behind in infotech capabilities, the internet has already stimulated creative possibilities for dissent. Web war has seen anti-government forces in Cambodia and Vietnam publicizing their protests. The Free Vietnam Alliance maintains http://www.fva.org based in Paris and Vietnam Insight (http://www.vinsight.org) in San Jose, California. Cambodian pro-democracy leader Sam Rainsy's "small party organization" maintains a home page (http://www.kreative.net/knp) containing "graphic photographs of anti-government demonstrators and other people killed in attacks blamed on Hun Sen".[32]

Malaysia. Aside from the ambitious Multimedia Super Corridor, Malaysia's economic growth and relations with Singapore shape the country's infotech plans and programs. Criticized for lacking "comprehensive total defence philosophy or infowar methodology",[33] Malaysia's defense establishment promises to go beyond computer virus infestations and reflect on "the new realities faced by Governments, businesses and communities as they moved on-line and became increasingly reliant on computer networks".[34]

Singapore. Singapore has Malaysia in mind because of its heavy dependence on its neighbor for vital needs such as water. Bereft of ability for defense in depth, Singapore had already prepared an integrared approach to its defense systems. Called Total Defense, it involves "Psychological Defence, Social Defence, Economic Defence, Civil Defence and Military Defence, involving all sectors and levels in Singapore".[35] As early as 1995, Singapore had already promised the army's battle preparedness, thanks to information technology, with "significantly improved lethality, survivability, speed, versatility, and sustainability".[36]

Philippines. A vibrant civil society and uncivil elements have both utilized the available technology to test the limits of expression and liability in the Philippines. They have both demonized public and private figures and institutions. Such a situation like the "love bug" controversy failed to confine the issue to the legal arena but may have also emboldened the nefarious activities. Philippine internal security forces have had their taste of cyber vandalism as the police web site was hacked but other examples of electronic fraud have remained confidential.[37] Computer-based disaster and emergency response and sea transport surveillance systems have been unevenly utilized in keeping civilian death tolls down. Their security counterparts have been annoyingly embroiled in the embattled political landscape.

Socio-Cultural Transformation

Transformation in Southeast Asia—miraculous or otherwise—has yet to account completely for the role of the young, the Chinese community, or the middle classes in social change. Each of these social groups seems to play important parts unknown in societies elsewhere. One may suspect that they are both separately or collectively evolving new social institutions that can pave the way for a libertarian setup that matches the requirements of informatized segments of societies.

New social relations will certainly be engendered by novel modes of acquiring information and they will make the forces of the information revolution more deeply embedded in the available spaces for discourse, dissent and disposition. In this, the state may maximize such opportunities for broadening participation in democratic processes, as well as asserting national sovereignty and territorial integrity. The society-state nexus may thus be helped by the construction of bridges for engagement and negotiation. Meanwhile, the broad issues of social well-being and changes in the production and distribution of goods and services may unsettle the unitiated segments of the society. The neo-liberal market-driven thrusts, especially in the poorer parts of Southeast Asia, may dim hopes of utilizing information technology for combatting poverty and underdevelopment. The sum of evolving social relations is thus being constructed, negotiated and mediated by an increasing number of individuals, groups, sectors and classes accessing the benefits of the information revolution. Social movements can take the concrete form of informatized societies in modern Southeast Asia.

No doubt, revolutionary political openings have rendered state and nonstate actors highly visible and vulnerable in the unfolding information drama in southeast Asia. But the smoldering circumstances of Indonesia, Burma, Cambodia, Vietnam and the Philippines all point to transformative agendas that are increasingly helped by the ICT revolution. Revolutions in social relations are overturning traditional and orthodox ideas about social change mostly swept under the rug by regimes kept in power by their laws and their armies.[38] By themselves, these considerations can postpone the outbreak of all-out information warfare. Predictably, the escalation of information warfare in Southeast Asia will have to do more with the developments in the rest of the Asia-Pacific region because even this early we have seen how some countries have already engaged China in skirmishes.

Northeast Asia

No doubt, information warfare developments in Southeast Asia are very much connected with the developments in Northeast Asia by way of China and Taiwan and, to some extent, Japan. Despite China's scorecard in the latest Information Society Index, it is China together with Taiwan which has demonstrated the most developments in the doctrine and practice of information warfare as part of its "unrestricted warfare." China and Taiwan's great ICT advantages seem to fan the flames of cyber conflict in Asia in general. As Bickers notes:

> If Asia is the cyberwarrior's proving ground, then the key battleground is the Taiwan Strait. Observers say the struggle between China and Taiwan over Taiwanese sovereignty is the source of large-scale growth in cyberwar activities.

Exercises by China's PLA in July, simulating war on Taiwan, included cyberwar tactics, according to official Chinese media reports. "China's really at the forefront in the region, and Taiwan would be second," says Herman Finley, information-warfare specialist and associate professor at the U.S. military's Asia Pacific Centre for Security Studies in Honolulu. "It's not easy to get detail on China. However, they have created a number of schools including four universities within the PLA" specializing in information warfare.[39]

China's ICT capabilities have been amply shown against Taiwan and the US in a variety of ways, including a May 4th movement cyberwarfare

campaign (vandalizing the official White House website) to redress the bombing of its embassy in Belgrade. On another retaliatory, but silent, incident Bill Bennett wrote in June 2001:

> When Chinese authorities impounded a US spy plane following a mid-air incident in April, American programmers retaliated immediately with an unprecedented series of attacks on Chinese websites. Within hours, the Honkers Union of China - a group of hackers - responded in kind. In the days that followed, the rival gangs defaced hundreds of websites on both sides of the Pacific.[40]

Meanwhile, Taiwan is not to be outdone as its strategic agencies develop their own capabilities. South Korea too is cause for concern, something that may elevate the matter to a transnational threat. Consider the report that of the sources of cyber attacks last year, South Korea "topped the list with 34% of attacks, followed by China (29%), Japan (10%), Taiwan (7%), Hong Kong (4%), Australia (3%), India (2%), and Singapore (2%). By contrast, non-Pacific Rim countries posed a considerably lower threat profile, with Great Britain producing 7% of worldwide attacks and Germany (2%)".[41]

China has a history of disputes with a number of Southeast Asian countries, mostly over territorial claims in the South China Sea. While China has time and time again reassured these countries of its willingness to resolve the issues peacefully, none can assure that the conflict will not find another venue for antagonism, say, cyberspace. Other security-related concerns may cloud and sour the relations between China and Southeast Asia such that actors on either side may take initiatives that could send wrong signals to the other side. While China may reserve the right to clarify its intentions on a bilateral basis, as it usually does, Southeast Asian countries may deem it best to cooperate in matters relating to the advent of information warfare.[42]

Conclusions

Information warfare, in its many forms, has been manifest in Southeast Asia with the coming of the ICT. The experiences of these countries have varied greatly, shaped especially by the circumstances of the development efforts in each country. Most countries push IT-related programs at the level of social capital and investment promotion schemes. But only

Singapore and Malaysia seem to fulfill the battlefield transparency—in the sense of network-centric warfare—requirement of enhancing IT capability and its use in warfare, while other countries have yet to publicize their involvement in information warfare programs.

The world wide web visibility of Southeast Asian countries has prompted numerous examples of hack attacks and vandalisms but this can be explained not so much by reference to the levels of ICT development but attempts by civil-uncivil society groups seeking redress of grievances or expressing popular dissent against less than responsive regimes. This points to the fact that social relations have yet to evolve in Southeast Asia in ways that could truly hold the powerful to account for adequate expressions of voice to promote the desirable outcomes attendant to informatized societies. By and large, there is no open, massive and continuing information warfare in Southeast Asia. But developments in Northeast Asia, especially the fractious relations between China and Taiwan, may have implications for Southeast Asia that could influence the turn of information warfare events in the region. ❁

Endnotes

1 Bickers, Charles. "Combat on the Web." Extracts from the *Far Eastern Economic Review*. 16 August 2001. At http://netforce.mn/cybercombat.htm.

2 See, for example, Maynes, Charles William. "The World in the Year 2000: Prospects for Order or Disorder." Strategic Studies Institute. March 1993. At http://www.carlisle.army.mil/ssi/pubs/1993/nature/nature.pdf

3 Kluver, Randy. "Globalization, Informatization, and Intercultural Communication." 2000. At http://unpan1.un.org/intradoc/groups/public/documents/apcity-/unpan002006.htm

4 Stein, George. *Battlefield of the Future: 21st Century Warfare Issues*. Maxwell AFB, Ala.: Air University Press, September 1995. At http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html

5 Baumard, Philippe. "From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift." Paper presented at the Fourth International Conference on Information Warfare: Defining the European Perspective, Bruxelles, Belgique, 23-24 May 1996. Published in A. Campen, D. Dearth, R. Gooden (editors), *Cyberwar: Security, Strategy and Conflict in the Information Age*, Fairfax, Virginia: Armed Forces Communications and Electronics Association, International Press, 1996, pp. 147-160. Available on-line at http://www.iae.univ-aix.fr/cv/baumard/infowar_warfare.htm

6 Libicki, Martin. *What is Information Warfare?* ACIS Paper 3. Washington DC: National Defense University. August 1995. At http://www.ndu.edu/inss/libicki.html; Copley, Gregor. "Re-defining Psychological Strategy in the Age of Information Warfare." *Defense & Foreign Affairs Strategic Policy* 26:6 (June 1998), pp. 5-8.

7 Singh, Jasbir. "Najib outlines cyberspace threat to military networks." Posted on InfoSec News isn@c4i.org. 11 June 2002.

8 Yoshihara, Toshi. "Chinese Information Warfare: A Phantom Menace or Emerging Threat?" Carlisle, PA.: US Army/Strategic Studies Institute. November 2001. At http://carlisle-www.army.mil/usassi/welcome.htm.

9 See Kopp, Carlo. Information Warfare: 1.A Fundamental Paradigm of Infowar 2.Issues in Current Infowar, Technical Report. 6 January 2002; Mengxion, Chang. Weapons Of The 21st Century The Revolution In Military Affairs. Part Four. N.d. At http://www.ndu.edu/inss/books/chinview/chinapt4.html.

10 Burke, Martin. *Information Superiority, Network Centric Warfare and the Knowledge Edge*. Salisbury: Defense Science and Technology Organization (Australia), 2000, p. 3; Burke, Martin. "Information Superiority Is Insufficient To Win In Network Centric Warfare." 2000. At http://www.dodccrp.org/2000ICCRTS/cd/papers/Track4/024.pdf. See also Newland, Ronald ."Tactical Deception in Information Warfare: A New Paradigm for C4I." *Journal of Electronic Defense* 21:12 (December 1998), pp. 43-48.

11 Anderson, Kent. "Intelligence-Based Threat Assessments for Information Networks and Infrastructures: A White Paper." 11 March 1998 (Revised 25 January 1999). At http://www.aracnet.com/~kea/Papers/threat_white_paper.shtml.

12 Ortis, Cameron and Paul Evans. "The Internet and Asia-Pacific Security: Encountering the 'Dark Side'." Prepared for the international symposium on "Electronic Media, Markets and Civil Society in East and Southeast Asia." City University of Hong Kong. 15-16 April 2002 (draft manuscript).

13 Christensen, John. "Bracing for Guerrilla Warfare in Cyberspace." 6 April 1999. *At* http://www.cnn.com/TECH/specials/hackers/cyberterror/; Lim, Jamus Jerome and Yap Ching Wi. "Taming the Hydra: The Impact of ICT in the Asia Pacific." 2002. At http://econ.ucsc.edu/grads/jamus/paper9.pdf; McDonald, Tim. "Fanatics with Laptops: The Coming Cyber War." 16 May 2002. At http://www.news-channels.com/articles/ceb7-f21ebf749a0c816dd2d6b39a4608.htm.

14 BBC. "Hack attacks on rise in Asia." 7 November 2002. At http://news.bbc.co.uk/2/hi/-technology/2415795.stm

15 UNCTAD-UNESCAP. Joint Asia-Pacific Regional Conference on E-Commerce Strategies for Development. Bangkok. 20-22 November 2002 Final Report: Topical Sessions. At http://r0.unctad.org/ecommerce/event_docs/bangkok_final.pdf

16 See, for example, Thuvasethakul, Chadamas and Thaweesak Koanantakool. "National ICT Policy in Thailand." Presented at Africa-Asia Workshop Promoting Co-operation in Information and Communications Technologies Development. Kuala Lumpur and Penang, Malaysia. 25-29 March 2002. At http://www.nectec.or.th/users/htk/publish/20020302-National-ICT-Policy-v16-word.pdf; Arroyo, Gloria Macapagal. "Speech during the Visit to the 7th e-ASEAN Task Force." Oakwook Premier Hotel, Ayala Center, Makati City. 20 April 2001. At http://www.opnet.ops.gov.ph/speech-2001april20.htm.

17 Moore, Nick . "The Information Policy Agenda in East Asia." Paper prepared for a seminar held at the British Library. 1996. At http://www.acumenuk.co.uk/paper2.html.

18 Evans, Robert . "Broadband booms in rich nations." Reuters. 16 September 2003; Shannon, Victoria. "Surfers shift to an Internet built for speed." *International Herald Tribune*. September 17, 2003. At http://www.iht.com

19 Chai, Winston. "Security can't Stop Asian Hackers." CNETAsia. May 27, 2003. At http://zdnet.com.com/2100-1105_2-1010044.html.

20 VNA, "Embracing the Information Age." 7 January 2002. At http://vietnamnews.vnagency.com.vn/2002-01/05/Stories/13.htm.

21 Kahler, Miles. "Information Networks and Global Politics." 1999. At http://www.mpp-rdg.mpg.de/pdf_dat/kahler.pdf.

22 See, Ch'ng Kim. "Government Information and Information about Governments in Southeast Asia: A New Era? An Overview." *Inspel* 35: 2(2001), pp. 120-136

23 Eng, Peter. "A New Kind Of Cyberwar In Burma, Thailand, Indonesia, Vietnam: Bloodless Conflict. "*Columbia Journalism Review*. September-October 1998. At http://www.hartford-hwp.com/archives/54/233.html.

24 "Okkar." "The New light of Myanmar: Current Status and Prospect of IT Application in Myanmar." Soc.culture. burma. 2 July, 2002. Posted by "Okkar" okkar66126@yahoo.com.

25 Glave, James. "Cyber 'Vandals' Target Indonesia." 18 August 1998.

26 BBC. "Hack attacks on rise in Asia." 7 November 2002. At http://news.bbc.co.uk/2/hi/-technology/2415795.stm

27 See also Pabico, Alecks. "The Internet, A Handy Political Weapon." Interpress News Service. 14 January 1999.

28 McKay, Niall. "Indonesia, Ireland in Info War?" At http://www.wired.com/news/politics/0,1283,17562,00.html. 27 January 1999.

29 Sallot, Jeff. "Timorese 'Hacktivists' Warn of Revenge: Exiled Resistance Leader Threatens to Launch Cyber Attacks on Indonesian Computer Targets." *The Globe and Mail*. 28 August 1999.

30 Eng, same as above n 23.

31 Gellman, Barton. "Cyber-Attacks by Al Qaeda Feared." *Washington Post*. 27 June 2002.

32 Eng, same as above n 23.

33 Kwan, Edmund. "Whither Cyber War between Malaysia and Singapore ?" Paper Presented at Infowarcon '97. Vienna. 11 September 1997, p. 6. At http://www.infowar.com/iwcon/KwanWord6.doc

34 Najib Razak in Singh, Jasbir. "Najib outlines cyberspace threat to military networks." Posted on InfoSec News isn@c4i.org. 11 June 2002.

35 Kwan, same as above n 32.

36 Cited in Tan, Andrew. "Singapore's Defence: Capabilities, Trends and Implications." *Contemporary Southeast Asia* 21:3 (December 1999), p. 466.

37 Oliva, Erwin Lemuel. "PNP Seeks Selp from ePLDT Following Hacker Attacks." 6 March 2003 At http://www.inq7.net/inf/2003/mar/07/inf_1-1.htm).

38 Edappagath, Ajmal and Eun-Ju Kim. "Legal and Regulatory Awareness of the ICT - Identifying Solutions for Cybercrimes." *Business Briefing: Global Info Security*. 2002; see alo Aldrich, Richard. "The International Legal Implications of Information Warfare." *Airpower Journal*. Fall 1996. pp. 99-110.

39 Bickers, Charles. "Combat on the Web." Extracts from the *Far Eastern Economic Review*. 16 August 2001. At http://netforce.mn/cybercombat.htm.

40 Bennett, Bill. "US-China cyberwar wasn't isolated incident." 20 June 2001. At http://afr.com/specialreports/report3/2001/06/20/FFXNUX8P1OC.html).

41 Predictive Systems. "After U.S., South Korea Produced Most Cyber-Attacks In Q4 2001. Study." 2002. At http://www.predictive.com; Power, Richard. "2002 CSI/FBI Computer Crime and Security Survey." Computer Security: Issues and Trend 8:1 (Spring 2002) http://www.gocsi.com; Riptech. "Riptech Internet Security Threat Report: *Attack Trends for Q3 and Q4 2001*," January 2002.

42 Xinhua. (China News Agency). "China Defense White Paper." 2002.

References

Aldrich, Richard. "The International Legal Implications of Information Warfare." *Airpower Journal*. Fall 1996. pp. 99-110.

Anderson, Kent. "Intelligence-Based Threat Assessments for Information Networks and Infrastructures: A White Paper." 11 March 1998 (Revised 25 January 1999). At http://www.aracnet.com/~kea/Papers/threat_white_paper.shtml.

Arroyo, Gloria Macapagal. "Speech during the Visit to the 7th e-ASEAN Task Force." Oakwook Premier Hotel, Ayala Center, Makati City. 20 April 2001. At http://www.opnet.ops.gov.ph/speech-2001april20.htm

Baumard, Philippe. "From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift." Paper presented at the Fourth International Conference on Information Warfare: Defining the European Perspective, Bruxelles. Belgique. 23-24 May 1996. Published in A. Campen, D. Dearth, R. Gooden (editors), *Cyberwar: Security, Strategy and Conflict in the Information Age*, Fairfax, Virginia: Armed Forces Communications and Electronics Association, International Press, 1996, pp. 147-160. Available online at http://www.iae.univ-aix.fr/cv/baumard/infowar_warfare.htm

BBC. "Hack attacks on rise in Asia." 7 November 2002. At http://news.bbc.co.uk/2/hi/-technology/2415795.stm

Bennett, Bill. "US-China cyberwar wasn't isolated incident." 20 June 2001. At http://afr.com/specialreports/report3/2001/06/20/FFXNUX8P10C.html)

Bickers, Charles. "Combat on the Web." Extracts from the *Far Eastern Economic Review*. 16 August 2001. At http://netforce.mn/cybercombat.htm.

Burke, Martin. *Information Superiority, Network Centric Warfare and the Knowledge Edge*. Salisbury: Defense Science and Technology Organization (Australia), 2000.

_____. "Information Superiority is Insufficient To Win In Network Centric Warfare." 2000. At http://www.dodccrp.org/2000ICCRTS/cd/papers/Track4/024.pdf

Chai, Winston. "Security can't Stop Asian Hackers." CNETAsia. May 27, 2003. At http://zdnet.com.com/2100-1105_2-1010044.html.

Christensen, John. "Bracing for Guerrilla Warfare in Cyberspace." 6 April 1999. At http://www.cnn.com/TECH/specials/hackers/cyberterror/.

Copley, Gregor. "Re-defining Psychological Strategy in the Age of Information Warfare." *Defense & Foreign Affairs Strategic Policy* 26:6 (June 1998), pp. 5-8.

Edappagath, Ajmal and Eun-Ju Kim. "Legal and Regulatory Awareness of the ICT - Identifying Solutions for Cybercrimes." *Business Briefing: Global Info Security*. 2002.

Eng, Peter. "A New Kind Of Cyberwar In Burma, Thailand, Indonesia, Vietnam: Bloodless Conflict. "*Columbia Journalism Review*. September-October 1998. At http://www.hartford-hwp.com/archives/54/233.html.

Evans, Robert . "Broadband booms in rich nations." Reuters. 16 September 2003.

Gellman, Barton. "Cyber-Attacks by Al Qaeda Feared." *Washington Post*. 27 June 2002.

Glave, James. "Cyber 'Vandals' Target Indonesia." 18 August 1998.

IT Reporters. "Thailand's daily news Web site hacked." 30 December 2000.

"Junta Hackers Spread Virus." *Far Eastern Economic Review*. 10 February 2000.

Kahler, Miles. "Information Networks and Global Politics." 1999. At http://www.mpp-rdg.mpg.de/pdf_dat/kahler.pdf.

Kluver, Randy. "Globalization, Informatization, and Intercultural Communication." 2000. At http://unpan1.un.org/intradoc/groups/public/documents/apcity-/unpan002006.htm

Kopp, Carlo. *Information Warfare: 1.A Fundamental Paradigm of Infowar 2.Issues in Current Infowar, Technical Report*. 6 January 2002.

Kwan, Edmund. "Whither Cyber War between Malaysia and Singapore ?" Paper Presented at Infowarcon '97. Vienna. 11 September 1997. At http://www.infowar.com/iwcon/KwanWord6.doc

Libicki, Martin. *What Is Information Warfare?* ACIS Paper 3. Washington DC: National Defense University. August 1995. At http://www.ndu.edu/inss/libicki.html

Lim, Jamus Jerome and Yap Ching Wi. "Taming the Hydra: The Impact of ICT in the Asia Pacific." 2002. At http://econ.ucsc.edu/grads/jamus/paper9.pdf

"Listening Post." *Far Easter Economic Review*. September 18, 1997. Posted at http://www.burmanet.org/burmanet/1997/Bnet820.txt.

Maynes, Charles William. "The World in the Year 2000: Prospects for Order or Disorder." Strategic Studies Institute. March 1993. At http://www.carlisle.army.mil/ssi/pubs/1993/nature/nature.pdf

McDonald, Tim. "Fanatics with Laptops: The Coming Cyber War." 16 May 2002. At http://www.news-channels.com/articles/ceb7-f21ebf749a0c816dd2d6b39a4608.htm

McKay, Niall. "Indonesia, Ireland in Info War?" 27 January 1999. At http://www.wired.com/news/politics/0,1283,17562,00.html

Mengxion, *Chang. Weapons Of The 21st Century The Revolution In Military Affairs*. Part Four. N.d. At http://www.ndu.edu/inss/books/chinview/chinapt4.html.

Moore, Nick . "The Information Policy Agenda in East Asia." Paper prepared for a seminar held at the British Library. 1996. At http://www.acumenuk.co.uk/paper2.html

Newland, Ronald ."Tactical Deception in Information Warfare: A New Paradigm for C4I." *Journal of Electronic Defense* 21:12 (December 1998), pp. 43-48. (via Proquest)

Oliva, Erwin Lemuel. "PNP Seeks Selp from ePLDT Following Hacker Attacks." 6 March 2003 At http://www.inq7.net/inf/2003/mar/07/inf_1-1.htm).

Ortis, Cameron and Paul Evans. "The Internet and Asia-Pacific Security: Encountering the 'Dark Side'." Prepared for the international symposium on "Electronic Media, Markets and Civil Society in East and Southeast Asia," City University of Hong Kong. 15-16 April 2002 (draft manuscript).

"Okkar." "The New light of Myanmar: Current Status and Prospect of IT Application in Myanmar." Soc.culture. burma. 2 July, 2002. Posted by "Okkar" okkar66126@yahoo.com.

Pabico, Alecks. "The Internet, A Handy Political Weapon." Interpress News Service. 14 January 1999.

Predictive Systems. "After U.S., South Korea Produced Most Cyber-Attacks In Q4 2001. Study." 2002. At http://www.predictive.com.

Power, Richard. "2002 CSI/FBI Computer Crime and Security Survey," Computer Security: Issues and Trend 8:1 (Spring 2002) http://www.gocsi.com;

Riptech. "Riptech Internet Security Threat Report: *Attack Trends for Q3 and Q4 2001*," January 2002

Sailot, Jeff. "Timorese 'Hacktivists' Warn of Revenge: Exiled Resistance Leader Threatens to Launch Cyber Attacks on Indonesian Computer Targets." *The Globe and Mail*. 28 August 1999.

See, Ch'ng Kim. "Government Information and Information about Governments in Southeast Asia: A New Era? An Overview." *Inspel* 35: 2(2001), pp. 120-136

Singh, Ajay. "Information Warfare: Reshaping Traditional Perceptions." n.d. At http://www.idsa-india.org/an-mar-4.html.

Singh, Jasbir. "Najib outlines cyberspace threat to military networks." Posted on InfoSec News isn@c4i.org. 11 June 2002.

Shannon, Victoria. "Surfers shift to an Internet built for speed." *International Herald Tribune*. September 17, 2003. At http://www.iht.com

Stein, George. *Battlefield of the Future: 21st Century Warfare Issues*. Maxwell AFB, Ala.: Air University Press, September 1995. At http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html

Tan, Andrew. "Singapore's Defence: Capabilities, Trends and Implications." *Contemporary Southeast Asia* 21:3 (December 1999), pp. 451-474.

Tedjabayu. "Indonesia: The Net as a Weapon." Presented at the Asian Journalists' Seminar in Subic Bay, Philippines, 1998. Rewritten for "Next Five Minutes Tactical Media Conference in Amsterdam." 12-14 March 1999. *CyberSociology* Magazine Issue 5. At http://www.socio.demon.co.uk/magazine/5/5indonesia.html

Thuvasethakul, Chadamas and Thaweesak Koanantakool. "National ICT Policy in Thailand." Presented at Africa-Asia Workshop Promoting Co-operation in Information and Communications Technologies Development. Kuala Lumpur and Penang, Malaysia. 25-29 March 2002. At http://www.nectec.or.th/users/htk/publish/20020302-National-ICT-Policy-v16-word.pdf

Tseng, Jang-ruey. "The PRC's Research on Information Warfare, Its Influence over the ROC and the ROC's Counter-measures." Taiwan Research Institute, Division of Strategic and International Studies. February 2000.

UNCTAD-UNESCAP. Joint Asia-Pacific Regional Conference on E-Commerce Strategies for Development. Bangkok. 20-22 November 2002 Final Report - Topical Sessions. At http://r0.unctad.org/ecommerce/event_docs/bangkok_final.pdf

Urbas, Gregor. *Cybercrime Legislation in the Asia-Pacific Region*. Australian Institute of Criminology. 2001. At http://www.hku.hk/crime/).

VNA. "Embracing the Information Age." 7 January 2002. At http://vietnamnews.vnagency.com.vn/2002-01/05/Stories/13.htm

Yoshihara, Toshi. "Chinese Information Warfare: A Phantom Menace or Emerging Threat?" Carlisle, PA.: US Army/Strategic Studies Institute. November 2001. At http://carlisle-www.army.mil/usassi/welcome.htm.

Xinhua. (China News Agency). "China Defense White Paper." 2002.