No. 104

The LTTE's Online Network and its Implications for Regional Security

Shyam Tekwani

JANUARY 2006

With Compliments

Institute of Defence and Strategic Studies
Singapore

This Working Paper is part of a series of studies on Non-Traditional Security in Southeast Asia. It has been produced under a grant from the Ford Foundation, for which the Institute of Defence and Strategic Studies gratefully acknowledges.

The Institute of Defence and Strategic Studies (IDSS) was established in July 1996 as an autonomous research institute within the Nanyang Technological University. Its objectives are to:

- Conduct research on security, strategic and international issues.
- Provide general and graduate education in strategic studies, international relations, defence management and defence technology.
- Promote joint and exchange programmes with similar regional and international institutions; organise seminars/conferences on topics salient to the strategic and policy communities of the Asia-Pacific.

Constituents of IDSS include the International Centre for Political Violence and Terrorism Research (ICPVTR) and the Asian Programme for Negotiation and Conflict Management (APNCM).

Research

Through its Working Paper Series, *IDSS Commentaries* and other publications, the Institute seeks to share its research findings with the strategic studies and defence policy communities. The Institute's researchers are also encouraged to publish their writings in refereed journals. The focus of research is on issues relating to the security and stability of the Asia-Pacific region and their implications for Singapore and other countries in the region. The Institute has also established the S. Rajaratnam Professorship in Strategic Studies (named after Singapore's first Foreign Minister), to bring distinguished scholars to participate in the work of the Institute. Previous holders of the Chair include Professors Stephen Walt (Harvard University), Jack Snyder (Columbia University), Wang Jisi (Chinese Academy of Social Sciences), Alastair Iain Johnston (Harvard University) and John Mearsheimer (University of Chicago). A Visiting Research Fellow Programme also enables overseas scholars to carry out related research in the Institute.

Teaching

The Institute provides educational opportunities at an advanced level to professionals from both the private and public sectors in Singapore as well as overseas through graduate programmes, namely, the Master of Science in Strategic Studies, the Master of Science in International Relations and the Master of Science in International Political Economy. These programmes are conducted full-time and part-time by an international faculty. The Institute also has a Doctoral programme for research in these fields of study. In addition to these graduate programmes, the Institute also teaches various modules in courses conducted by the SAFTI Military Institute, SAF Warrant Officers' School, Civil Defence Academy, Singapore Technologies College, and the Defence and Home Affairs Ministries. The Institute also runs a one-semester course on '*The International Relations of the Asia Pacific'* for undergraduates in NTU.

Networking

The Institute convenes workshops, seminars and colloquia on aspects of international relations and security development that are of contemporary and historical significance. Highlights of the Institute's activities include a regular Colloquium on Strategic Trends in the 21st Century, the annual Asia Pacific Programme for Senior Military Officers (APPSMO) and the biennial Asia Pacific Security Conference (held in conjunction with Asian Aerospace). IDSS staff participate in Track II security dialogues and scholarly conferences in the Asia-Pacific. IDSS has contacts and collaborations with many international think tanks and research institutes throughout Asia, Europe and the United States. The Institute has also participated in research projects funded by the Ford Foundation and the Sasakawa Peace Foundation. It also serves as the Secretariat for the Council for Security Cooperation in the Asia-Pacific (CSCAP), Singapore. Through these activities, the Institute aims to develop and nurture a network of researchers whose collaborative efforts will yield new insights into security issues of interest to Singapore and the region

ABSTRACT

In the light of the expanding online networks of terrorist groups and the immediate and foreseeable threat they represent both to the sovereignty of nations and the security of the critical and informational infrastructures, the case for securitization of the internet is a valid and urgent one. This paper will use the case study of the online network of the LTTE to demonstrate how online networks pose a security threat and how securitization of the internet can offer solutions.

****

Shyam Tekwani lectures in the School of Communication & Information, at Nanyang Technological University, Singapore. He is a photojournalist turned academic who spent over a decade covering conflict and terrorism from the frontlines in South Asia. His current work focuses on the adaptability of new media technologies by, and communication strategies of, non-state groups around the world.

The LTTE's Online Network and its Implications for Regional Security

Introduction

The Liberation Tigers of Tamil Eelam (LTTE) of Sri Lanka is consistently rated as Asia's most ruthless – and one of the world's deadliest - terror groups by terrorism experts and international security organisations. The group has used conventional, guerrilla, and terror tactics in a bloody, two-decade-old conflict that has claimed over 60,000 lives and displaced hundreds of thousands of Sri Lankans. From the early 1970s, the group has developed into a formidable fighting force having integrated a battlefield insurgent strategy with a terrorist program that targets key government and military personnel, the economy (the Central Bank and the Colombo World Trade Centre), and public infrastructure (commuter trains, buses, oil tanks, and power stations).

The only terrorist organisation in the world to have assassinated two national leaders - Sri Lankan President Ranasinghe Premadasa in 1993 and Indian Prime Minister Rajiv Gandhi in 1991 - the LTTE is the pioneer in its brutal genre. It was the LTTE that pioneered the use of suicide vests and used them to carry out far more suicide-bomb attacks (over 200), than any other terrorist organisation. The LTTE was among the first terrorist groups to adapt new media technologies such as the Internet to aid in its propaganda, funding and recruitment drives with a sophisticated and networked presence on the World Wide Web that spans the globe, drawing on the resources of the well entrenched Tamil Diaspora abroad. The LTTE mounted the world's first known cyber attack, when it swamped the Sri Lankan government's embassy networks in 1997.

Rationale for the importance of an analysis of LTTE

The LTTE's use of the Internet and other new media and communication technologies as an integral part of its campaign represents an emerging security issue in the region. Terrorism is increasingly finding a place in the international discourse on non-

traditional security. International terrorism is emerging as a critical security issue in Asia in particular with the recent terrorist attacks in Indonesia and the growing evidence of networked terrorist activity in the entire region. As the information revolution extends and deepens its impact in the region, and more Asians than ever have access to networked computers, the use of the internet by terrorists and insurgents demands the attention of academics and analysts across the world.

Although the LTTE is at the moment engaged in a very public negotiation process, amidst a ceasefire that has been the longest in the history of the ethnic conflict in Sri Lanka, the LTTE still poses a significant regional and international security threat. Not just because the LTTE has been using the quiet of the ceasefire to regroup and rearm. The factors facilitating such a perception also go beyond the regional political implications of what many regard as a highly successful separatist insurgency (what is on the offer on the peace table in Sri Lanka is little short of an independent state) and its impact on the sovereignty of Sri Lanka. More critical to the rapidly developing technological environment in the region are the long terms implications of the strategic and tactical operational innovations pioneered by the LTTE, including the transnational network operations, the networked internet presence and the consistently innovative terrorist strategies that will linger long after the LTTE fades from memory.

Securitization of the Internet

In the light of the expanding online networks of terrorist groups and the immediate and foreseeable threat they represent both to the sovereignty of nations and the security of the critical and informational infrastructures, the case for securitization of the internet is a valid and urgent one. This paper will use the case study of the online network of the LTTE to demonstrate how online networks pose a security threat and how securitization of the internet can offer solutions. Before describing the online networks of the LTTE and its security implications it is important to ground such a discussion within the framework of securitization and examine its relevance in contemporary practice.

Disruption of information infrastructure is increasingly seen as an option for non state actors who may not have the ability to match forces on a conventional battlefield. To counter this threat governments across the world are developing cyber strategies to protect such information infrastructures and command and control structures. Some governments, notably the United States are also devising strategies to prevent the proliferation of such crime and the growing level of online recruitment, communication and fundraising activity of non state actors. They are also formulating new laws and strengthening existing laws to curtail the online activities of non sate actors and prosecute perpetrators of cyber crime. While securitization of the Internet is a viable option, there are many hurdles. Notably, the nature of the online networks themselves, where security is hardly a part of network design. In addition, securitization of the Internet can never be a responsibility of governments alone, because most of the online networks are operated by the private sector even as they are controlled by the state. As Shelley has argued:

> Because information technology is primarily in the private sector, public private partnerships are needed to locate abuse of the Internet by transnational criminals. This may include network monitoring by private corporations to detect suspicious websites or usage patterns[1].

A large degree of cooperation between governments and the private sector will be called for. In addition, because the Internet is a virtual, borderless world, international cooperation, another complex issue, is a must. Shelley identifies cooperation between developed and developing countries as a key factor in tackling the internet and its security, as also citizen support in identifying problematic or suspicious websites. But no matter how complex the issues, they can be tackled with political will, and a systematic approach.

In what can be described as the first initiative towards delineating the Internet as a security issue, the US government came up in 2003 with a 'National Strategy to Secure Cyberspace' from which many of the strategies being considered by other nations to begin the process of dealing with the Internet as a security issue derives[2]. The US strategy describes itself as a framework for "protecting the (cyberspace)

[1] Louise I. Shelley, *Organized Crime, Terrorism and Cybercrime TraCCC*. Available at <www.american.edu/tracc>.
[2] *National Strategy to Secure Cyberspace*, February 2003, US Government document.

infrastructure that is essential to our economy, security, our way of life". The strategy describes cyberspace as the nervous system powering the country's critical infrastructures, protection of which is essential to its national security. The 60 page document is the first of its kind to identify cyberspace and internet security as a vital security concern comparable to other military and infrastructure concerns. Clearly the document is an outcome of the heightened concerns on internet security in the fallout of the September 11 attacks and the merging role of the Internet and new communications technologies in the planning, funding and executing of terrorist attacks, and the growing awareness of how modern day terrorist are using the internet as a networking tool.

Before moving on the securitization of the Internet and its implications it is important to identify the securitizing actors, referent objects and the relevant audience to locate the concept within the securitization framework.

Securitizing Actors: As in the case of transnational crime, the securitizing actors remain Heads of State and the foreign and interior ministers. Senior police chiefs and officials involved in dealing with transnational crime are also important securitizing actors. But because securitizing the internet involves the private sector as well, representatives of the technological elite such as leaders of private industry involved in internet design/security can be involved as securitizing actors.

Referent Objects: Unlike the bordered, boundaried sovereign state as the referent object in the securitization of transnational crime, the referent object in this case is cyberspace itself, the security/integrity of which being the prime objective of such a securitization.

Audience: The relevant audience is the entire online community which needs to be persuaded of the threat to both the networks' security and its uninterrupted, unimpeded existence and operation. This is especially important because any securitization of the Internet is bound to give rise to complex issues of freedom of information and expression, and privacy creating the need for extensive dialogue between securitizing actors and the audience. The audience could also include governments of developing countries, and governments of those countries with rigid

control on network use who need to be persuaded of the significance of the threat and the importance for international cooperation.

Terrorism in Asia

The U.S. State Department's annual publication on Patterns of Global Terrorism for 2002 notes that the incidents of terrorist attacks in Asia were on the rise since the dawn of this century (99 in 2002, 68 in 2001 and 99 in 2000) lending credence to the view held by many terrorism experts that the centre of terrorism's gravity has shifted to Asia. In 2002, South Asia remained a central battle-ground in the global war on transnational terrorism.

The Bali blasts and the bombing of a Jakarta hotel, both of which claimed many non-Asian victims have served to bring terrorism in the region higher up on many international agendas. The JI plot to target American interests in Singapore and emerging revelations about the presence of Al Qaeda in the region and its links to regional terrorist groups have precipitated the shifting of focus to terrorism in southeast Asia. International attention on the threat of terrorism in Asia took on a sharper edge since the attacks against the United States on September 11, 2001. Not only is this part of the heightened global awareness of terrorism as a critical non-traditional security issue, it also reflects the fact that nonstate actors based in the region are networked to one another and that they have transcended the confines of their geographical boundaries to be transnational players.

Terrorism in Asia is not a new phenomenon. The world's oldest ongoing insurgency, the Moro rebellion is still active in the Philippines. Other nonstate actors active in the region include the Jemaah Islamiyah in Indonesia and Malaysia, the various pro-Pakistan groups operating in Kashmir, the Maoist insurgency in Nepal, Aum Shinrikyo in Japan, Abu Sayyaf in the Philippines, the Uighurs in China, and the LTTE in Sri Lanka. Many of these groups have linkages to each other. Such transnational linkages cut across religious and political ideologies and geographic, ethnic and linguistic boundaries. Al Qaeda's linkages in the region are well documented in several instances, and are a critical element of any analysis of

terrorism in the region[3]. Just as Al Qaeda transfers funds and training to other groups in the region it also enables the percolation of its technological know how and communications strategies to its allies and franchisees. While Al Qaeda retains the centre stage on the international scene, it is a relatively recent phenomenon in the region, compared to the LTTE of Sri Lanka.

Terrorism and the information revolution

To understand the significance of the regional security threat posed by the LTTE it is necessary first to examine the relationship between terrorism and new media technologies. The information revolution in Asia offers terrorist groups the same benefits and advantages that it extends to business enterprises in the region. Increased globalization and rapid absorption of new media technologies into business practice has enabled the ongoing dynamic economic environment in many Asian nations. Just as business corporations in Asia are adapting their tactical and operational strategies to make the best use of new technology and the emerging global economy, extremist groups are doing the same. The rapid expansion of networked computers, internet café's, mobile phone services and other new media technologies is enhancing transnational linkages across the board. Transnational networks have existed long before the Internet - ancient Diasporas such as the Roma and the Jewish Diasporas have always formed networks to exchange information and goods. Terrorist groups have also maintained international networks long before the emergence of modern media technology. The LTTE's transnational networks date back to the early eighties with its reach extending through south Asia, eastern and Western Europe and North America to procure arms, smuggle narcotics and even trade in illegal aliens[4]. But

[3] See S. Reeve, *The New Jackals:Ramzi Yousef, Osama bin Laden and the Future of terrorism*, London: Andre Deutsch, 1999. Also see R. Gunaratna, *Inside Al Qaeda Global Network of terror*, UK: C. Hurst and Co., 2002.

[4] For comprehensive accounts of the LTTE's international networks and the ethnic conflict in Sri Lanka see the works of Rohan Gunaratna on the LTTE , including *Sri Lanka's Ethnic Conflict and National Security*, South Asian Network on Conflict Research, 1998; 'LTTE Fundraisers Still on the Offensive,' *Jane's Intelligence Review*, December 1997; *International and Regional Security Implications of the Sri Lankan Tamil Insurgency*, Alumni Association of the Bandaranaike Centre for International Studies, 1997.
For a useful overview also see P.Chalk, 'Liberation Tigers of Tamil Eelam's (LTTE) international organization and operations - a preliminary analysis,' *Commentary No. 77a Canadian Security Intelligence Service* publication, 1999, Winter. Available at:

modern technology, combined with increased international migration patterns, the advent of modern transportation and the increased globalization of international commerce, the means of networking have become quicker, cheaper, more covert and more varied. Raids on terrorist hideouts across the globe, from bombed out houses in Afghanistan to apartments in Metro Manila, routinely yield laptop computers, digital video equipment, digital photographs, CD-ROMs and encrypted diskettes. The information revolution has contributed to the ability of terrorist groups in the region to network with others to form transnational networks that cooperate in disseminating propaganda and fundraising and recruitment. It has also enhanced their ability to coordinate and carry out attacks across international borders.

Just as mom and pop stores and local coffee shops across the world are being edged out by international conglomerates such as Walmart and Starbucks, small, local terrorist groups with limited funds and membership and a geographically specific, limited theater of operation are making way for transnational networks such as LTTE, Al Qaeda and HAMAS. In a study of trends in Middle-eastern terrorism, Zanini found that modern communications technologies such as the Internet have facilitated the evolution of terrorist groups into multi-organizational network incorporating informational technology into their operational tactics[5]. Whine posited that new media technologies are enabling a shift from 'absolute hierarchies to hydra headed networks' which are harder to defeat[6]. The new environment favors transnational networks over local terrorist groups. In fact there is no such thing as a local terrorist group or a local terrorist threat anymore. The local terrorist threat is now not just a regional one but a global one.

An emerging body of literature is documenting the growing use of new media technologies such as the internet, digital media technologies such as digicams and CD-ROMs and satellite communications systems. This emergent trend complements the traditional use of media by terrorists. Publicity has always been a central goal of terrorists, and they use the media to publicize their actions to the widest possible

---

<http://www.csisscrs.gc.ca/eng/comment/com77_e.html>. Another interesting account is that of A. Davis, 'Tigers Inc,' *Asia Week*. Available at <http://www.realityofsrilanka.com/Asia-week.htm>.

[5] Michele Zanini, *Middle Eastern Terrorism and Netwar Studies in Conflict and Terrorism,* 22,1999: 247-56.

[6] Michael Whine, 'Cyberspace - A New Medium for Communication, Command, and Control,' *Studies in Conflict and Terrorism*, 22, 1999: 231-45.

audience to create the maximum fear and confusion; to mobilize support and public opinion and to aid recruitment and fundraising[7].

With the advent of the new media technologies such as the Internet, terrorist groups have also become more sophisticated in their use of media and media tools. The Internet, mobile phones and new satellite technology enable dispersed groups and nodes of larger networked groups to stay in touch over distance. Many diasporic groups also use the Internet to support terrorist movements by providing political support in the form of propaganda and lobbying international public opinion[8]. They also help raise funds and offer logistical support to militants[9].

With the advent of the World Wide Web, now accessible from the remotest corners of Asia through Internet cafes and the expansion of telecommunications networks, terrorists do not have to depend on other media to carry their messages to their target audiences. They can now use the Internet to present 'news' and views, and use their own video and audio tapes to enhance their presentations. The online networks, consisting of several interlinked websites on the Internet are a constantly updated archive for terrorist ideologies and propaganda to which an international audience comprising active supporters and sympathizers, diasporas, media, and the general public are increasingly referring to for background information as well as news updates.

Besides using the Internet to spread propaganda, terrorists can be said to use the Internet for the following:

a) *Intra and Inter group communication:* The Internet enables dispersed members of terrorist groups to communicate with each other covertly, and anonymously. Networked terrorist groups also use the internet to communicate

[7] For a more detailed discussion on the relationship between media and terrorism, see B. Hoffman, *Inside Terrorism*, London: Victor Gollancz, 1998, p. 131. Also See Paul Wilkinson, 'Media and Terrorism - A reassessment,' *Terrorism and Political Violence*, Vol. 19, No 2, Summer 1997: 51-64.
[8] S.Tekwani, "The Tamil Diaspora, Tamil Militancy, and the Internet," in K.C. Ho, R. Kluver, & K.C.C. Yang (eds), *Asia.com:Asia Encounters the Internet*, London & New York: RoutledgeCurzon, 2003, pp. 175-92.
[9] Louise I. Shelley, *Organized Crime, Terrorism and Cybercrime TraCCC*. Available at <www.american.edu/traccc>.

with other groups sharing similar goals. Email is now believed to have played an important role in coordinating the attacks of September 11.

b) *Linking diasporic group to militant networks:* Diasporic groups settled outside their homelands are usually educated and computer literate, using the Internet to keep in touch with co ethnics abroad as well as the home country. The diasporic Asians are known to use the Internet to keep abreast of news from home and to network with others from their community. Many diasporic groups, such as the Sri Lankan Tamils also use the Internet to support terrorist movements by providing political support in the form of propaganda and lobbying international public opinion. The role of the Burmese Diaspora in bringing pressure on the International business community is a documented case in point[10]. They also help raise funds and offer logistical support to militants.

c) *Framing news and actions:* The Internet also enables the terrorists to frame their actions and their ideologies in the manner of their choice without the intervention of government or media censors. Through their web sites terrorist groups can now frame their ideologies and their actions to suit their needs and the political and social environment they function in. The Internet enables terrorists to focus their message on their cause rather than the actions reported in the mass media. The LTTE website for instance can (and does) highlight gruesome images of Sri Lankan army attacks on 'Tamil civilians', not equally brutal images of LTTE suicide bombing victims.

The Internet allows terrorists to tailor audience specific messages for specific audiences. Many LTTE Tamil language sites carry images and text tailored specifically for Tamil audiences. Aleph's Japanese language sites have more in common with the Aum Shinrikyo of old that it is trying to publicly disassociate itself from, than its English language site which is focused on distancing itself from the crimes of its erstwhile leader - Asahara. The Islamic Jihad Web site which is available in English and in Arabic uses a similar ploy. The English site is a propaganda site

[10] See T. Danitz and W. Strobel, 'Networking Dissent:Cyber Activists use the Internet to Promote Democracy in Burma,' in J. Arquilla and D. Ronfeldt (eds), *Networks and Netwars*, RAND 2001, pp.129-69.

which does not dwell on the group's bloody exploits. But the Arabic site is a paean to martyrs, or shahids, who during attacks on Israelis[11].

The LTTE Network

Brief word on Origins and development

The Liberation Tigers of Tamil Eelam grew out of a radical Tamil nationalist movement that emerged in the 1970s to counter perceived discrimination by the Sinhalese majority. While other Tamil nationalists favoured political approaches to securing autonomy, the LTTE took to arms killing 13 Sri Lankan soldiers in 1983 which sparked the civil war that continues today. The LTTE controls about a quarter of Sri Lanka's territory.

In seeking a separate state, Eelam, in Sri Lanka, the LTTE has used conventional, guerrilla, and terror tactics, that include over 200 suicide bombings, in a bloody, two-decade-old civil war that has claimed more than 60,000 lives and displaced hundreds of thousands in Sri Lanka.

The leader, Velupillai Prabhakaran, is credited with turning the LTTE into a formidable rebel army. The LTTE's chief negotiator and political adviser is Anton Balasingham, a former Sri Lankan journalist who has dabbled in Marxism-Leninism.

Experts call the LTTE one of the best-financed terrorist groups in the world, due to the group's fund-raising and propaganda network among sympathetic Tamils in North America, Europe, Asia, and Australia. It also reportedly makes money through trafficking in drugs and arms.

[11] T. Lightly and S. Franklin, *Activist targets Jihad's Web site*, January 5, 2003. Available at <http://www.chicagotribune.com/technology/chi-0301050233jan05,1,6016350.story?coll=chi%2Dtechtopheds%2Dhed> (Accessed on 24 September 2003).

International network

A cover story in Asia Week magazine called it the LTTE International Inc. or Tigers Inc., referring to the international network of 'commercial companies and small businesses, informal banking channels, a fleet of ships, political offices, aid and human rights organizations, arms dealers and foreign mercenaries[12]' that form the formidable network of the LTTE spanning the globe engaged in disseminating propaganda, raising funds a and procuring arms.

With the emergence of the Internet and other communication technologies following in the wake of globalization of commerce and the information revolution a whole body of literature has been spawned on the transition of organizations, both legitimate business corporations and terrorist outfits, from hierarchies to networks. The LTTE in a sense has always been a network. It has always maintained separate networks and personnel for separate functions. LTTE leader Prabhakaran in fact functions much like a multinational CEO, overseeing operations from the top, while personnel and networks he has in place carry out their functions largely independent of each other. Thus there is one network based largely in the west, heavily involved with the Tamil Diaspora that is responsible for the LTTE's propaganda campaign. Other clandestine networks are active in the Asian region engaged in more criminal activities from arms procurement to illegal fund raising.

LTTE's international propaganda machinery, previously coordinated through its main office in London, is now primarily centered on its online campaign through a vast interlinked network maintained by LTTE members and members of the Tamil Diaspora all over the world. The changing political environment with regard to the LTTE in particular, which is now proscribed in many of its previous havens such as India, the UK , the US and Australia; as well as the post Sep-11 war on terrorism, have combined to drive the LTTE's networks into a more clandestine mode. It is important to note here that the LTTE has been forced, in recent years, by mounting international pressure, to move its more criminal enterprises such as arms smuggling, and many believe drug running and people smuggling, to South and South East Asia

[12] Anthony Davis, see note 1.

where the prevailing lax legal environment is more conducive to its activities. The emergence of the Internet however, has enabled the group to continue to coordinate its key propaganda network from bases in the western world, which are critical, both in terms of providing the LTTE with the critical technological infrastructure to do so as well as to keep international public opinion focused on its political campaign. It also enables the Sri Lankan Tamil Diaspora which lives in large numbers in Western countries to actively participate and extend the LTTE's own propaganda campaign. The Internet in this context has emerged as a viable alternative, affording cheap, accessible and conveniently covert modes of operation that has replaced and in some instances supplements the preexisting network.

The LTTE's formidable online presence is a virtual Tamil Eelam online.

The group's main website eelam.com claims:

> 'The Tamil people of the island of Ceylon (now called Sri Lanka) constitute a distinct nation. They form a social entity, with their own history, traditions, culture, language and traditional homeland. The Tamil people call their nation Tamil Eelam.' [13]

Diaspora Sri Lankan Tamils can now read Eelam newspapers; listen to Eelam Radio; mail Eelam e-cards showing Eelam maps and flags to friends on festive occasions; listen to tapes of their 'national leader's' speeches; and refer to online yellow pages and web directories for information on Eelam Tamils. Online newsgroups and e-forums on Tamil websites offer a platform for discussions on the Tamil struggle for a separate state and a showcase for the history, culture, traditions and politics of the Tamils of Sri Lanka. In addition to the websites hosted by the LTTE, pro-LTTE and pro-Eelam sites, personal homepages maintained by expatriate Tamils in cities and universities across the western world provide virtual Eelam and its citizens a dynamic and very visible presence on the World Wide Web. So visible and vibrant that Sri Lankan Tamils are said to 'inhabit a cyberspace Eelam'[14].

[13] Available at <http://www.eelam.com>
[14] ibid.

LTTE Online

The Eelam network online is a complex interlinked web of sites that together represent a virtual Tamil nation, at the political center of which is the LTTE, and its supreme commander Prabhakaran, referred to as the "national leader'. The core of the online network consists of the political sites that represent the LTTE and the Tamil nation it claims to represent. Many of these are regarded as 'official sites' and are maintained by the LTTE. These function very much like the government sites of other legitimate nations. Replete with the insignia of 'Eelam' government such as flags, maps and pictures of Prabhakaran, the 'national Leader" these sites provide an up to date version of the ongoing military campaign, and strive to reinforce the 'suffering' of the Tamils and the 'sacrifices' of the LTTE guerillas, using text-articles of historical analysis, accounts of the struggle, biographies of martyrs, descriptions of the majority Sinhalese's acts of oppression and discrimination. The sites often carry graphic photographs of civilian casualties inflicted by the Sri Lanka Army, photographs of LTTE 'martyrs', and images from victorious military campaigns. An example is footage of the Sri Lankan Army's most humiliating defeats: the September 1998 Battle of Kilinochchi. The army's attempt to capture to establish a land route from Kandy, in the south-central highlands, to Jaffna, in the north, lasted well over 500 days and ended in the deaths of over 600 Sri Lankan soldiers. Stills from this footage can be downloaded off the site.

EelamWeb. Com, one of the main LTTE sites, claims that it "is aimed at rebuilding Tamil Eelam, the traditional home land of the Tamils, which has been ravaged by the genocidal policies that have been undertaken by successive Sinhala dominated Sri Lankan governments'.

Another site, http://www.infoeelam.com/aboutus.htm, described as the 'Gateway to Tamil Eelam', claims, "our main mission here to promote Tamil Eelam to the World Stage and to act as a central source of Tamil Eelam related information to all of our people". http://www.tamilmaravan.com/ is a site dedicated to the members of the LTTE who died either in suicide bombing missions or other more militaristic campaigns against the Sri Lankan army.11443 Tamil 'martyrs' are named on this site and there are almost as many photographs of the dead. Other similar sites include:

http://thamileelam.org, http://www.eelamnation.com/, TamilPower.com and Sangam.org.

In keeping with its claimed status as a 'nation' Eelam (or the LTTE) maintains a 'government' presence on the through sites such as that of the LTTE Peace Secretariat at http://www.lttepeacesecretariat.com which puts out 'communiqués' intended to keep aloft the notion that the LTTE really wants peace and that war has been forced upon it by the actions of the Sinhala-majority government. www.teedor.org/ is the site of the Tamil Eelam Economic Development Organization, representing various administrative departments of Eelam, to be implemented on the ground when Eelam becomes a physical reality. By many accounts Teedor is also a semi-operational in LTTE controlled territory in Northeast Sri Lanka, although many believe such bodies are only a fundraising front for the LTTE war chest[15]. Teedor's departments include Hardware, Software, Tamil Software, Energy, and Agriculture. Animal Husbandry, Commerce and Energy. Other sites in this category include those of other, smaller organizations operating under the broader 'Tamil' umbrella such as the Student Organizations of the World Tamil Movement site available at: http://www.mediaicon.com/sowtm/tamil_eelam.htm.

Tamil Diaspora Sites

The Sri Lankan Tamil Diaspora is an important element in the LTTE's political and military campaign. Commentators and observers of the LTTE and its campaigns have frequently pointed out the significant role played by the Diaspora in funneling funds to the LTTE campaign and often functioning as active nodes in the extended LTTE network[16]. The Diaspora's contribution to the LTTE's online network is no less significant. The Tamil Diaspora is one of the most networked and its members are

[15] See Rohan Gunaratna, *Sri Lanka's Ethnic Conflict and National Security*; Rohan Gunaratna, 'LTTE Fundraisers Still on the Offensive'; Rohan Gunaratna, *International and Regional Security Implications of the Sri Lankan Tamil Insurgency*; P. Chalk, 'Liberation Tigers of Tamil Eelam's (LTTE) international organization and operations - a preliminary analysis.'

[16] See B.Nichiporuk, *The security Implications of demographic factors*, RAND Corp, 2000. See especially pages 21-23. Available at <http://www.rand.org/publications/MR/MR1088/MR1088.html.> Also see B. Nichiporuk and C.H. Builder, 'Societal Implications,' in J. Arquilla and D. Ronfeldt (eds), *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND, 1997.

extensive users of the Internet, using the medium to communicate with each other and to receive updates on news from the embattled Northeast of Sri Lanka.

Tamilcanadian.com, which describes itself as a site for the 'History and culture of Tamils of Tamil Eelam is one of the dominant Diaspora sites.' Talking Point, is a popular and highly active Diaspora discussion group hosted on the Tamilcanadian.com site, where a broad spectrum of expatriate Tamils from across the globe comment and discuss a variety of issues pertaining to the politics of Sri Lanka and the outcome of the ongoing war (Subramanian, 2000). It is regarded as among the most influential of the Diaspora sites. Others include:http://www.eelam.dk. (Denmark), www.tamilnet.net.au (Australia), and tesoc.com/ (Tamil Eelam Society of Canada).

The Internet has been an important medium for Sri Lankan Tamils abroad as the media in Sri Lanka is government controlled and through the ethnic conflict both local and international media have been subjected to strict censorship. The Internet has emerged as an important vehicle for the LTTE to circumvent such censorship and put out its own version of the war and simultaneously it enables the Tamil Diaspora to receive news from Tamil rather than Sinhalese, or perceivably pro-government news sources. This quest for news from home has driven the Diaspora Tamils to be innovative in their pursuit of news sources and channels. The Tamil network now has a plethora of sites and technologies to choose from-audio print and video news is available round the clock from a variety of sources, many sites use the latest MP3 technology. Information out of Jaffna, the heart of Tamil country, and the center of the war zone, which has no working telephone lines – is passed through word of mouth, ham-radio and via the Tamil Tigers clandestine radio station[17] which is now available on many Tamil websites. News thus channeled is distributed through the vast Tamil online network in various forms. Eelam.s5.com, is a comprehensive media site featuring links to Tamil newspapers, Tamil radio and the Tamil Internet.Tamilwebradio.com is a wholly audio site featuring news, speeches of Tamil leaders and Eelam songs. Jaffnanews, available at: http://www.jaffna.freehomepage.com, named after the capital of the Tamil northeast,

[17] Majumder, BBC Online.

is another news based site. In addition, there are several Tamil newspapers online which have names and formats similar to mainstream newspapers in their host countries which also provide news from home and updates on the war in addition to local information pertaining to the cultural life of Diasporas. These include: www.Tamil Guardian.com Online and the Tamil Tribune at http://www.geocities.com/tamiltribune.

Besides a network of general sites that link Tamils across the globe such as Tamilcyber and Jaffnatamils online or colombotamils online, there are numerous sites pertaining to the life of the Diaspora in the host country, highlighting the culture of Tamils, their history, entertainment, and social life. These sites serve to reinforce a sense of community and belonging among the dispersed Tamils and linking and cross-linking across political and geographic boundaries. They also serve up the visual and tangible symbols of Eelam eagerly sought after by immigrant communities yearning for home. These include information sites featuring directories and links for Tamils living abroad, online stores selling Eelam and LTTE memorabilia, from posters, cards, audio and video tapes, flags and T-shirts; to sites dedicated to Eelam music, or e-cards.

Some of these sites are:
www.yarl.com/ecards/gbrowse.php?cat_id=14. This is an online store selling e-cards with pictures of Prabhakaran, and other living and dead leaders of the LTTE such as Kittu, Maps, Flags, and LTTE soldiers in fetching fatigues.
www.maxpages.com/eezamnation/EelamSongs is dedicated to patriotic and propagandistic songs on Tamil culture and the Eelam struggle which one can listen to and download online.
http://www.tamiltigers.net/eelambooks/flyers/flyers_about_tamil_eelam.htm is another propaganda site selling books and pamphlets on Eelam and the LTTE and the Tamil movement. Eelavar Networks is a directory service serving as an online directory for Tamils. Its slug line is "Changing the way eelavar communicate"[18] and consists of a Yellow pages listing of Tamils as well as an international Web Directory on Tamils and Tamil links.Besides the above listed major sites there are several Tamil

[18] Eelavar-is a Tamil word used to mean '(those) of Eelam' or people of Eelam.

language sites which offer similar variations of the English language sites to a staunch Tamil audience. These include sites such as: http://tamilhistory.hypermart.net/eelam.html; Eelathamilar.com; Thamilnaatham.com; Digitamil.cjb.net; and Thamileelam.dk.

While it is apparent that the online network is primarily used for propaganda purposes serving up a dynamic and vibrant Tamil presence, offering emotional and cultural sustenance to Diaspora Tamils and an outlet for political discourse they may have otherwise been denied, the online network is also a symbol of a parallel network that runs on more subterranean lines, channeling funds, recruits and arms to the LTTE.

Underscoring the often intangible link between diaspora activism and militancy, and at another level the transfer of technology enabled by diaspora involvement, is the Vannitech Institute in the embattled North east of Sri Lanka inaugurated last year with much fanfare. Conceived, funded and run by Tamil expatriate knowhow and financial inputs, the institute, which has been set up to usher in the new era of infotech to the undeveloped North east, was opened with an inaugural function that was dominated by LTTE brass including S.P. Tamilselvan, head of the political wing of the LTTE and Illamkumaran, head of the educational organization of Tamil Eelam. What this shows is that the lines between separatism and social networking are blurred in the case of Sri Lanka and the new technology makes such distinctions even less visible.

Securitizing the Internet

The Internet and its use by terrorists in their campaigns, both as a tool of communication and propaganda and a target of terrorist attacks is only beginning to be discussed in academic circles. Most such discussion focuses on scenarios of cyber terrorism and envisages coordinated attacks on critical computer infrastructures, and data bases that are seen as having the potential to cripple governments and databases[19]. These are far fetched scenarios as of today requiring a degree of expertise

[19] See the works of Dorothy Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, sponsored by the Nautilus Institute, Fall 1999. Available at

in computers as yet unavailable to terrorist groups in the region. Further, such attacks are more likely in highly developed societies more dependant on computer systems. It may happen in the future as youth who are products of a technology driven culture are inducted into the ranks of terrorists[20]. In the current time, the internet is primarily an enabling technology, useful as a propaganda vehicle and a valuable covert communication tool, increasingly useful in planning operations.

The Internet was largely perceived by many analysts as being a useful publicity tool and no more. The events of Sep 11th have served to some extent in altering these views and ushering in the perception that the Internet represents a whole new world of potential for terrorists, insurgencies and anti-government campaigns across the globe. An Al Qaeda front organization, Al- farouq, published a newly written book on its website entitled:" The 39 Principles of Jihad"[21] Principle 34 is entitled 'Performing electronic Jihad' and calls for believers to join the Jihad by participating in Internet forums to defend Islam and the Mujahideen, to preach Jihad and to encourage Muslims to learn more about Jihad. The Internet is described as providing an opportunity to reach vast, target audiences and respond swiftly to false allegations. Computer experts are asked to use their skills to destroy American, Jewish and secular websites among others. Since the attacks of Sep 11th and the reports of the role played by the Internet in the coordination of these attacks, however unsubstantiated, words such as steganography and web encryption have come into popular parlance. The use of email and satellite phones by Al Qaeda and the use of the Internet by HAMAS are on the other hand well documented[22]. Hoffman describes Osama Bin Laden as a 'terrorist CEO' running Al Qaeda like a multinational corporation[23]. Prabhakaran presides over yet another multinational corporation with equally diverse business interests. Just as MNC's have adapted their modes of operations to best avail of the advantage of new technologies to reduce operational costs and enhance productivity so too have the terrorism CEOs. From websites and email to sophisticated audio and

---

<http://www.nautilus.org/info-policy/workshop/papers/denning.html>. Also see J. Hasham, *Emerging Threats on the Internet*, 2000. Available at <http://www.ciaonet.org/pbei/riia/jom01.html>.

[20] J.M. Post, G.R. Ruby, E.D. Shaw, 'From Car Bombs to Logic Bombs: The Growing Threat of Information Terrorism,' *Terrorism and Political Violence*, Vol.12, No.2, Summer, 2000: 97-122.

[21] Mohammad Bin Ahmad Al-Salem,*39 wasila Li-Khidmat Al-Jihad Wa- Al-Musharaka Fihi*, 2003 Available at <http://www.faroq.net/news/>.

[22] Whine Zanini. See notes 2 and 3.

[23] B. Hoffman, 'Rethinking Terrorism and Counter-terrorism since 9/11,' *Studies in Conflict & Terrorism*, 25, 2002: 303–316, p. 308.

video enhancements of online multimedia presentations, terrorist groups in the region are investing considerable expertise and effort on their new media dimension. The MILF, LTTE, Islamic Jihad, Aleph, Lashkar eToiba (LeT) are just some Asian groups making extensive use of media and communication technologies to obtain their political and tactical goals.

In this context the Internet is as much a potential security issue as any offline terrorist network such as the Al Qaeda's hawala currency network or the LTTE's arms procurement network.

The political implications of an insurgency such as the LTTE's have been discussed for some years now. There is an abundance of literature on the implications of a separate Tamil state to the political stability of the region and that of Sri Lanka, if such a time were to come to pass[24].What is less discussed is the implications of the online network of the LTTE. The LTTE's pioneering use of the internet in Asia; South Asia in particular is an emerging security issue in a region that is experiencing a significant government driven surge in Internet connectivity, without a parallel development of a legal framework to deal with such issues.

According to the United Nations World Development Report (UNWDR), in 1990 there were only six telephone lines per 1,000 people in Indonesia, 10 in the Philippines, 24 in Thailand, 89 in Malaysia and 385 in Singapore. By 2001 the statistics had changed dramatically, with the number of lines per 1,000 people rising to 35 in Indonesia, 42 in the Philippines, 99 in Thailand, 198 in Malaysia and 562 in Singapore. Asia accounts for 36 per cent of the world's telecom Market, a figure that is expected to go up to 50 per cent in 2007; it has 33 per cent of the worlds Internet user base and seven of the worlds Top Ten most profitable telecom operators[25]. While most of these statistics are dominated by countries such as South Korea, Singapore and Japan, Philippines, Indonesia and Malaysia are high on the list of countries which

[24] A useful starting point is K. Jayawardhana, *Ethnic Conflict in Sri Lanka and Regional Security*, 1987. Available at <http://www.infolanka.com/org/srilanka/issues/kumari.htm>. Also see R.I. Rotberg (ed.), *Creating peace in Sri Lanka : civil war and reconciliation*, Cambridge, Mass.: World Peace Foundation and Belfer Center for Science and International Affairs, Washington, D.C., Brookings Institution Press, 1999.
[25] UNDP Report 2003. Available at <http://www.undp.org/hdr2003/pdf/hdr03_HDI.pdf>.

have a rapidly growing user-base for computers, Internet services and mobile phones. As the know- how percolates down to groups in the southeast Asia the technology is becoming more easily available within the region, allowing for easy adoption of new tools by terrorists.

The Sri Lankan government which many perceive having lost the propaganda war with LTTE even more thoroughly than it has the war on the ground, has no infrastructure, legal or technical, to block access to LTTE and pro LTTE sites within Sri Lanka even though the entire media-print, radio and broadcast are under strict government control. This is a loophole the LTTE has used well. In a related matter the creator of the I Love You virus, in the Philippines got way unpunished because the Philippines government had no laws in place to prosecute cyber crimes. The situation is depressingly similar across Asia with the exception of perhaps Singapore. Asian nations are getting on to the information highway without any traffic laws in place. Just as online business ventures in Asia are seen as potentially risky and unstable, as evidenced by the dotcom crash of the nineties, the unpatrolled navigation of the internet by terrorists is a potential security threat.

The US government has clearly identified the Internet as a security issue, the protection of which is essential to the security of the nation itself, and has begun the process of identifying strategies and policies to protect its informational and economic infrastructures online. This is a definite outcome of the 9/11 attacks and the underlying network vulnerability the attacks exposed. Governments across the world are now aware that there is a need to formalize the protection of information networks in much the same way as they safeguard national borders. Vesting the issue with a formal framework for securitization can only begin the complex process of identifying, problem areas, collaborations and cooperation strategies, between the public and private sectors, the developed and less developed world, the information rich and the information poor.

Conclusions

Asia is an emerging hotbed for terrorist activity. Besides the Middle eastern and Afghan groups who have links with various Islamic groups in the region such as the MILF and the Abu Sayyaf in Philippines, the JI in Indonesia and Malaysia, there are the South Asian groups such as the pro-Pakistan Kashmiri groups operating out of Pakistan and the LTTE in Sri Lanka who also have a regional presence through their arms procurement and other networks. All these regional groups are also extensive users of media technology, new and old. From websites and email to sophisticated audio and video enhancements of online presentations, these groups are investing considerable expertise and effort on their new media dimension. In the current environment where transnational organizations transfer knowledge and technology, much like their multinational business counterparts transfers of media technology know-how may well become routine exchanges between groups. These exchanges of propaganda, technology, training and funds are serving to fuel terrorist activity in the region. As Post et al pointed out, every new innovation in terrorism from car-bombs to suicide bombs have quickly spread through the world, with groups adept at copying each other and adapting to new trends[26]. The LTTE was one of the first groups to use the Internet in its campaigns, today almost every terrorist group, both in the region and across the world maintains a web presence, and uses the Internet in a variety of ways.

And as newer and more information technology oriented strategies evolve and are adopted into practice they will not only be copied by other groups, they will also be distributed through electronic mail, mailing lists, and newsgroups, which act as a repository of collective information, keeping all parties informed of all new developments[27]. In such an environment it is imperative that the internet plays a more important role in the non traditional security discourse. Such a move is particularly critical in the region where the biggest boom in the information revolution is expected

[26] J.M. Post, G.R. Ruby and E.D. Shaw, 'From Car Bombs to Logic Bombs: The Growing Threat of Information Terrorism.'

[27] Michael Wilson, *Terrorism in a New World--Evolution in Revolution*.
Available at < http://www.emergency.com/evo-revo.htm>.

to take place in countries which are least prepared with the necessary legal infrastructure and the policy framework to confront it.

Traditionally, security has been defined as military defense of territory, within a state system whose chief characteristic is a competition for security based upon (primarily military) power. This concept has evolved in recent years to include, apart from the conventional military and political issues, a variety of economic, social and environmental issues, broadly defined under the umbrella of non-traditional security. Terrorism is now regarded as a non-traditional security issue, and in the current global environment is a pre eminent issue of concern. However, in this era of globalization, and multilayered economic, social and political linkages enabled beyond geographical, cultural and political boundaries by the Internet and other new media and communication technologies spawned by the ongoing information revolution, the Internet itself is emerging as a security issue. In as much as it enables the new global, social and economic order, the Internet also emerges as a key vulnerability, spawning a variety of security issues-related to the vulnerability of computerized societies to internet enabled crime. With its potential for various uses by terrorist for inter and intra group communications and propaganda as outlined above, and the envisaged scenarios of cyber terrorism in the future, to hacking, spamming, unleashing of viruses, invasion of databases and critical infrastructures linked to the Internet, theft of identity, and assorted crime for profit perpetrated online, the Internet exposes key vulnerabilities of individuals, corporations and nations. Especially in Asia where the legal and policy framework consistently lags behind the government driven drive towards Internet expansion.

A case demonstrating the urgency the issue merits is that of the creator of the I Love You virus which infected over 50 million computers across the world and caused over 6 billion dollars in damages to international business. Reomel Ramones, an ex-student of Manila's Computer College, who was arrested by Manila police after they traced him through IP logs and caller identification with help from the FBI, had to be released because the Philippines had no laws existing against computer crime. Investigators were forced to fall back on to offline laws governing credit card fraud and theft in order to charge the student. Among those hit by the virus, which, to prove a point further, originated from a nondescript apartment in a poorer part of a crowded

city in South East Asia, were countless governments, the Pentagon, major corporations such as Ford, Time Warner and the Microsoft. Ramones was charged with violating the Access Devices Regulation Act, which deals primarily with passwords for credit cards. Computer hacking at the time was not a crime under Philippine law. Since then the Philippines has some laws in place, but most of the rest of Asia is still vulnerable. While the I Love You bug was not the act of a terrorist, it exposes the underlying vulnerabilities of Asia's legal systems and underscores the urgency the issue calls for.

Experts predict that it is a matter of time before terrorists raised in the information culture and well versed in its technological aspects use a combination of computer borne and on the ground guerrilla tactics to amplify the damages in their attacks. Ciluffo and Gergely term this a 'synergistic attack'[28]. Visualize a 9/11 scenario where an attack on the twin towers is carried out in concert with a virus or a hacking attack into the power grid or emergency services database of New York city. The resulting disaster would have been multiplied ten fold.

When Internet-enabled terrorism is tackled from within the framework of a non-traditional security issue, the benefits that accrue to nations such as Sri Lanka, which are faced with grave threats to their sovereignty, and have already experienced tremendous loss of human life, both military and civilian, and staggering economic setbacks, brought about by the long and bloody civil war, are significant. One of the main factors affecting the Sri Lankan military's handling of the LTTE has been dwindling morale, whittled away by the support the LTTE had garnered in its early years from the international community. This was in large part due to its international propaganda campaign, which capitalized on its status as a marginalized minority and used the propaganda to focus on the sufferings of Tamils rather than the violence of its own actions. The LTTE continues to do so with considerable success on the Internet.

In addition the LTTE has also ventured into cyber crime on occasion. The LTTE has used the Internet to hack into Sri Lankan government networks in1997, the first

[28] F.J. Ciluffo and C.H. Gergely, 'Information Warfare and Strategic Terrorism,' *Terrorism and Political Violence*, Vol. 9, No.1 Spring, 1997: 84-94.

recorded use of internet terrorism in the world by any conventional terrorist group[29]. A wing of the Tamil Tigers calling itself the Internet Black Tigers bombarded the Sri Lankan embassy and consulate networks with junk e-mails, up to 800 per day. This cyber-terrorist attack, which swamped embassy computers for two weeks, is reputedly the first ever reported by US intelligence officials. The LTTE is also reported to have used the Internet for criminal profit, as evidenced by the University of Sheffield case, which exposes the more serious issue of internet identity theft by terrorists. The Tigers were able to hack into Sheffield University in England in 1997, and use the university computer system to send their propaganda and to engage in fund raising. And they did it in a covert manner. Because they were able to capture legitimate user IDs and passwords of some well-respected academics of the university and then disseminate e-mail communications around the world, they used those legitimate e-mail accounts and asked people to send money to a charity in Sri Lanka[30]. While such instances are not yet the norm, they are undeniably the trend of the future. And the LTTE is nothing if not a trend setter in tactics.

Securitizing this issue invests it with a certain urgency, which creates the political environment to enable a better allocation of manpower and resources to tackle the issue at the government end. It will propel multilateral action at an international level to initiate a legal framework to protect nations and their computer networks, which are multiplying and expanding at a rapid rate, even as they protect people's right to privacy and information. It will enable the creation and functioning of international law enforcement personnel trained to investigate internet enabled terrorism. One informal multilateral effort with some success is a G8 initiative set up in January 1997 as a subgroup on High-Tech Crime. The small size of the member group and commonality of interests led to establishing a 24/7 network of policing; speedy communications between member countries. It also endorsed the training of law enforcement officers from member countries on detecting, preventing and investigating cyber crimes.

---

[29] D. Denning, *Internet and Terrorism*, Carnegie Endowment for Peace. Lecture Series: Balancing National Security and Civil Liberties in an Age of Networked Terrorism. Available at <http://www.ceip.org/files/events/events.asp?EventID=391>.

[30] Michael Vatis (Deputy Assistant Director and Chief, National Infrastructure Protection Center, Federal Bureau of Investigation), 'Cyber Terrorism and Information Warfare: Government Perspectives,' in Yonah Alexander and Michael S. Swetnam (eds), *Cyber Terrorism and Information Warfare*, Transnational Publishers Inc, 2001.

Just as American troops have been committed to the southern Philippines to train Filipino troops battling Abu Sayyaf, a similar need exists to train and assist cyber cops in Asia. There is an urgent need for international commitment to inform, educate and facilitate partnerships at an informal level first, working around local sensitivities and sensibilities. Creating incident databases is a good place to start. Success at this stage would lead to MOU's, formal treaties and the necessary legislations.

It is not only propaganda that needs to be addressed but also the manner in which groups network with each other to exchange tactics, and variety of information on everything from safe houses to weapons procurement to bomb making information. The Internet is a network without geographical boundaries, internet enabled terrorism can only be tackled by a multilateral, multinational approach that transcends national boundaries. Nations are cooperating internationally to destroy terrorist networks on the ground. Online networks are no less threatening.

IDSS Working Paper Series

1.	Vietnam-China Relations Since The End of The Cold War *Ang Cheng Guan*	(1998)
2.	Multilateral Security Cooperation in the Asia-Pacific Region: Prospects and Possibilities *Desmond Ball*	(1999)
3.	Reordering Asia: "Cooperative Security" or Concert of Powers? *Amitav Acharya*	(1999)
4.	The South China Sea Dispute re-visited *Ang Cheng Guan*	(1999)
5.	Continuity and Change In Malaysian Politics: Assessing the Buildup to the 1999-2000 General Elections *Joseph Liow Chin Yong*	(1999)
6.	'Humanitarian Intervention in Kosovo' as Justified, Executed and Mediated by NATO: Strategic Lessons for Singapore *Kumar Ramakrishna*	(2000)
7.	Taiwan's Future: Mongolia or Tibet? *Chien-peng (C.P.) Chung*	(2001)
8.	Asia-Pacific Diplomac*ies:* Reading Discontinuity in Late-Modern Diplomatic Practice *Tan See Seng*	(2001)
9.	Framing "South Asia": Whose Imagined Region? *Sinderpal Singh*	(2001)
10.	Explaining Indonesia's Relations with Singapore During the New Order Period: The Case of Regime Maintenance and Foreign Policy *Terence Lee Chek Liang*	(2001)
11.	Human Security: Discourse, Statecraft, Emancipation *Tan See Seng*	(2001)
12.	Globalization and its Implications for Southeast Asian Security: A Vietnamese Perspective *Nguyen Phuong Binh*	(2001)
13.	Framework for Autonomy in Southeast Asia's Plural Societies *Miriam Coronel Ferrer*	(2001)

14. Burma: Protracted Conflict, Governance and Non-Traditional Security Issues (2001)
Ananda Rajah

15. Natural Resources Management and Environmental Security in Southeast Asia: Case Study of Clean Water Supplies in Singapore (2001)
Kog Yue Choong

16. Crisis and Transformation: ASEAN in the New Era (2001)
Etel Solingen

17. Human Security: East Versus West? (2001)
Amitav Acharya

18. Asian Developing Countries and the Next Round of WTO Negotiations (2001)
Barry Desker

19. Multilateralism, Neo-liberalism and Security in Asia: The Role of the Asia Pacific Economic Co-operation Forum (2001)
Ian Taylor

20. Humanitarian Intervention and Peacekeeping as Issues for Asia-Pacific Security (2001)
Derek McDougall

21. Comprehensive Security: The South Asian Case (2002)
S.D. Muni

22. The Evolution of China's Maritime Combat Doctrines and Models: 1949-2001 (2002)
You Ji

23. The Concept of Security Before and After September 11 (2002)
a. The Contested Concept of Security
Steve Smith
b. Security and Security Studies After September 11: Some Preliminary Reflections
Amitav Acharya

24. Democratisation In South Korea And Taiwan: The Effect Of Social Division On Inter-Korean and Cross-Strait Relations (2002)
Chien-peng (C.P.) Chung

25. Understanding Financial Globalisation (2002)
Andrew Walter

26. 911, American Praetorian Unilateralism and the Impact on State-Society Relations in Southeast Asia (2002)
Kumar Ramakrishna

27. Great Power Politics in Contemporary East Asia: Negotiating Multipolarity or Hegemony? (2002)
Tan See Seng

28. What Fear Hath Wrought: Missile Hysteria and The Writing of "America" (2002)
Tan See Seng

29. International Responses to Terrorism: The Limits and Possibilities of Legal Control of Terrorism by Regional Arrangement with Particular Reference to ASEAN (2002)
Ong Yen Nee

30. Reconceptualizing the PLA Navy in Post – Mao China: Functions, Warfare, Arms, and Organization (2002)
Nan Li

31. Attempting Developmental Regionalism Through AFTA: The Domestics Politics – Domestic Capital Nexus (2002)
Helen E S Nesadurai

32. 11 September and China: Opportunities, Challenges, and Warfighting (2002)
Nan Li

33. Islam and Society in Southeast Asia after September 11 (2002)
Barry Desker

34. Hegemonic Constraints: The Implications of September 11 For American Power (2002)
Evelyn Goh

35. Not Yet All Aboard…But Already All At Sea Over Container Security Initiative (2002)
Irvin Lim

36. Financial Liberalization and Prudential Regulation in East Asia: Still Perverse? (2002)
Andrew Walter

37. Indonesia and The Washington Consensus (2002)
Premjith Sadasivan

38. The Political Economy of FDI Location: Why Don't Political Checks and Balances and Treaty Constraints Matter? (2002)
Andrew Walter

39. The Securitization of Transnational Crime in ASEAN (2002)
Ralf Emmers

40. Liquidity Support and The Financial Crisis: The Indonesian Experience (2002)
J Soedradjad Djiwandono

41. A UK Perspective on Defence Equipment Acquisition (2003)
David Kirkpatrick

42. Regionalisation of Peace in Asia: Experiences and Prospects of ASEAN, ARF and UN Partnership (2003)
Mely C. Anthony

43. The WTO In 2003: Structural Shifts, State-Of-Play And Prospects For The Doha Round (2003)
Razeen Sally

44. Seeking Security In The Dragon's Shadow: China and Southeast Asia In The Emerging Asian Order (2003)
Amitav Acharya

45. Deconstructing Political Islam In Malaysia: UMNO'S Response To PAS' Religio-Political Dialectic (2003)
Joseph Liow

46. The War On Terror And The Future of Indonesian Democracy (2003)
Tatik S. Hafidz

47. Examining The Role of Foreign Assistance in Security Sector Reforms: The Indonesian Case (2003)
Eduardo Lachica

48. Sovereignty and The Politics of Identity in International Relations (2003)
Adrian Kuah

49. Deconstructing Jihad; Southeast Asia Contexts (2003)
Patricia Martinez

50. The Correlates of Nationalism in Beijing Public Opinion (2003)
Alastair Iain Johnston

51. In Search of Suitable Positions' in the Asia Pacific: Negotiating the US-China Relationship and Regional Security (2003)
Evelyn Goh

52. American Unilaterism, Foreign Economic Policy and the 'Securitisation' of Globalisation (2003)
Richard Higgott

53. Fireball on the Water: Naval Force Protection-Projection, Coast Guarding, Customs Border Security & Multilateral Cooperation in Rolling Back the Global Waves of Terror from the Sea (2003)
Irvin Lim

54. Revisiting Responses To Power Preponderance: Going Beyond The Balancing-Bandwagoning Dichotomy (2003)
Chong Ja Ian

55. Pre-emption and Prevention: An Ethical and Legal Critique of the Bush Doctrine and Anticipatory Use of Force In Defence of the State (2003)
Malcolm Brailey

56. The Indo-Chinese Enlargement of ASEAN: Implications for Regional Economic Integration (2003)
Helen E S Nesadurai

57. The Advent of a New Way of War: Theory and Practice of Effects Based Operation (2003)
Joshua Ho

58. Critical Mass: Weighing in on Force Transformation & Speed Kills Post-Operation Iraqi Freedom (2004)
Irvin Lim

59. Force Modernisation Trends in Southeast Asia (2004)
Andrew Tan

60. Testing Alternative Responses to Power Preponderance: Buffering, Binding, Bonding and Beleaguering in the Real World (2004)
Chong Ja Ian

61. Outlook on the Indonesian Parliamentary Election 2004 (2004)
Irman G. Lanti

62. Globalization and Non-Traditional Security Issues: A Study of Human and Drug Trafficking in East Asia (2004)
Ralf Emmers

63. Outlook for Malaysia's 11th General Election (2004)
Joseph Liow

64. Not *Many* Jobs Take a Whole Army: Special Operations Forces and The Revolution in Military Affairs. (2004)
Malcolm Brailey

65. Technological Globalisation and Regional Security in East Asia (2004)
J.D. Kenneth Boutin

66. UAVs/UCAVS – Missions, Challenges, and Strategic Implications for Small and Medium Powers (2004)
Manjeet Singh Pardesi

67. Singapore's Reaction to Rising China: Deep Engagement and Strategic Adjustment (2004)
Evelyn Goh

68. The Shifting Of Maritime Power And The Implications For Maritime Security In East Asia (2004)
Joshua Ho

69. China In The Mekong River Basin: The Regional Security Implications of Resource Development On The Lancang Jiang (2004)
Evelyn Goh

70. Examining the Defence Industrialization-Economic Growth Relationship: The Case of Singapore (2004)
Adrian Kuah and Bernard Loo

71. "Constructing" The Jemaah Islamiyah Terrorist: A Preliminary Inquiry (2004)
Kumar Ramakrishna

72. Malaysia and The United States: Rejecting Dominance, Embracing Engagement (2004)
Helen E S Nesadurai

73. The Indonesian Military as a Professional Organization: Criteria and Ramifications for Reform (2005)
John Bradford

74. Martime Terrorism in Southeast Asia: A Risk Assessment (2005)
Catherine Zara Raymond

75. Southeast Asian Maritime Security In The Age Of Terror: Threats, Opportunity, And Charting The Course Forward (2005)
John Bradford

76. Deducing India's Grand Strategy of Regional Hegemony from Historical and Conceptual Perspectives (2005)
Manjeet Singh Pardesi

77. Towards Better Peace Processes: A Comparative Study of Attempts to Broker Peace with MNLF and GAM (2005)
S P Harish

78. Multilateralism, Sovereignty and Normative Change in World Politics (2005)
Amitav Acharya

79. The State and Religious Institutions in Muslim Societies (2005)
Riaz Hassan

80. On Being Religious: Patterns of Religious Commitment in Muslim Societies (2005)
Riaz Hassan

81. The Security of Regional Sea Lanes (2005)
Joshua Ho

82. Civil-Military Relationship and Reform in the Defence Industry (2005)
Arthur S Ding

83. How Bargaining Alters Outcomes: Bilateral Trade Negotiations and Bargaining Strategies (2005)
Deborah Elms

84. Great Powers and Southeast Asian Regional Security Strategies: Omni-enmeshment, Balancing and Hierarchical Order (2005)
Evelyn Goh

85. Global Jihad, Sectarianism and The Madrassahs in Pakistan (2005)
Ali Riaz

86. Autobiography, Politics and Ideology in Sayyid Qutb's Reading of the Qur'an (2005)
Umej Bhatia

87. Maritime Disputes in the South China Sea: Strategic and Diplomatic Status Quo (2005)
Ralf Emmers

88. China's Political Commissars and Commanders: Trends & Dynamics (2005)
Srikanth Kondapalli

89. Piracy in Southeast Asia (2005)
New Trends, Issues and Responses
Catherine Zara Raymond

90. Geopolitics, Grand Strategy and the Bush Doctrine (2005)
Simon Dalby

91. Local Elections and Democracy in Indonesia: The Case of the Riau Archipelago (2005)
Nanykung Choi

92. The Impact of RMA on Conventional Deterrence: A Theoretical Analysis (2005)
Manjeet Singh Pardesi

93 Africa and the Challenge of Globalisation (2005)
Jeffrey Herbst

94 The East Asian Experience: The Poverty of 'Picking Winners (2005
Barry Desker and Deborah Elms

95 Bandung And The Political Economy Of North-South Relations: Sowing The Seeds For Revisioning International Society (2005)
Helen E S Nesadurai

96 Re-conceptualising the Military-Industrial Complex: A General Systems Theory Approach (2005)
Adrian Kuah

97 Food Security and the Threat From Within: Rice Policy Reforms in the Philippines (2006)
Bruce Tolentino

98 Non-Traditional Security Issues: Securitisation of Transnational Crime in Asia (2006)
James Laki

99 Securitizing/Desecuritizing the Filipinos' 'Outward Migration Issue'in the Philippines' Relations with Other Asian Governments (2006)
José N. Franco, Jr.

100 Securitization Of Illegal Migration of Bangladeshis To India (2006)
Josy Joseph

101 Environmental Management and Conflict in Southeast Asia – Land Reclamation and its Political Impact (2006)
Kog Yue-Choong

102 Securitizing border-crossing: The case of marginalized stateless minorities in the Thai-Burma Borderlands (2006)
Mika Toyota

103 The Incidence of Corruption in India: Is the Neglect of Governance Endangering Human Security in South Asia? (2006)
Shabnam Mallick and Rajarshi Sen

104 The LTTE's Online Network and its Implications for Regional Security (2006)
Shyam Tekwani