Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT)
Ministry of Foreign Affairs, Malaysia
No. 516, Persiaran Mahameru
50480 Kuala Lumpur
MALAYSIA

Tel: (603) 2261 1900
Fax: (603) 2274 9487
Email: info@searcct.gov.my
Website: www.searcct.gov.my

SEARCCT'SSELECTION OF ARTICLES VOLUME 1 | 2013

SEARCCT'S

SELECTION OF ARTICLES

VOLUME 1

2013

SEARCCT
SOUTHEAST ASIA REGIONAL CENTRE
FOR COUNTER-TERRORISM
MINISTRY OF FOREIGN AFFAIRS, MALAYSIA

SEARCCT'S SELECTION OF ARTICLES VOLUME 1/2013

PUBLISHER
SOUTHEAST ASIA REGIONAL CENTRE FOR
COUNTER-TERRORISM (SEARCCT)
MINISTRY OF FOREIGN AFFAIRS, MALAYSIA
No. 516, Persiaran Mahameru
50480 Kuala Lumpur
MALAYSIA

Tel	:	(603) 2261 1900
Fax	:	(603) 2274 9487
Email	:	info@searcct.gov.my
Website	:	www.searcct.gov.my

First Published in 2013

SEARCCT is dedicated to advocating the understanding of issues pertaining to terrorism and contributing ideas for counter-terrorism policy. The Centre accomplishes this mainly by conducting capacity building courses, research, publications and public awareness programmes. ALL STATEMENTS OF FACT AND EXPRESSIONS OF OPINION CONTAINED IN THIS WORK IS THE SOLE RESPONSIBILITY OF THE AUTHOR. THE GOVERNMENT OF MALAYSIA ASSUMES NO RESPONSIBILITY OF ANY STATEMENT OF FACT OR OPINION EXPRESSED IN THIS WORK.

TABLE OF CONTENTS

ARTICLES

VISION

TO BE A REGIONAL CENTRE OF EXCELLENCE IN RESEARCH AND TRAINING ON COUNTER-TERRORISM

FOREWORD

Twelve years following one of the deadliest terrorist attacks in the history of mankind, followed by rigorous and amplified security cooperation at the local, regional and international levels, the world is still struggling to eradicate the threats posed by terrorist groups. But, what is more staggering is the fact that despite such intensified cooperation, these groups have shown a shrewd ability to adapt to the retaliatory actions against them and remain a grave threat to society.

Terrorists today are operating in much smaller networks and cells. Criminals housed in prisons are becoming more susceptible to radical ideologies while more individuals, especially youth, are being radicalised and recruited through the internet. Terrorists have also learned to adopt other non-conventional means of executing their activities including travelling via sea and the acquisition of dangerous chemicals such as cyanide and sarin. Therefore, counter-terrorism measures must also be designed to accommodate the changing nature of terrorism.

In light of this, it gives me great pleasure to put in your hands the first edition of the "Southeast Asia Regional Centre for Counter Terrorism's (SEARCCT) Selection of Articles" for the year 2013.

This edition is specifically designed to enhance the knowledge of enforcement, security and government officials on the current issues of terrorism and counter-terrorism that spans across the Asian continent. It attempts to discuss several existing issues from the current state of Nepal, following the Nepali Civil War, to what motivates the disadvantaged population of Pakistan to engage in suicide attacks. In addition, it also explores the issues of terrorism in the Southeast Asian region, the growing exploitation of the media and the internet as well as the roles of relevant agencies in combating terrorism.

I would like to convey my heartfelt appreciation to our dedicated writers who have shown their unwavering support for SEARCCT and their willingness to share their knowledge and experience with our readers, to the Research and Publication Division of SEARCCT for overseeing the completion of this piece and to Dr. Rekha Nair who did an exceptional job in editing the monograph.

My sincere gratitude also goes to the Honourable Dato' Sri Anifah Hj. Aman, Minsiter of Foreign Affairs, Malaysia and Tan Sri Mohd. Radzi Abdul Rahman, Secretary General of the Ministry of Foreign Affairs, Malaysia for their unstinting support and encouragement for this endeavor.

Lastly, to the readers of this monograph, it is my sincere hope that the collection of articles presented in this edition will stimulate your enthusiasm and help nurture creative yet practical ways to counter the evolving threats of terrorism. As stated so succinctly by the famous 19th century writer, Anton Chekov, "knowledge is of no value until you put it into practise."

Thank you.

DATIN PADUKA RASHIDAH RAMLI
Director-General
Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT)
Ministry of Foreign Affairs, Malaysia.

A THEORETICAL FRAMEWORK FOR UNDERSTANDING RADICALISATION INTO VIOLENT EXTREMISM[1]

Kumar Ramakhrisna

ABSTRACT

Ten years since the Bali bombings of October 2002 that killed 202 civilians, the threat of violent extremism remains significant and of concern to many governments in Southeast Asia and beyond. The United Kingdom's well-known Contest Strategy, for instance has long pointed out the need to find ways to counter "violent extremism."[2] *In August 2011, moreover, the Obama Administration affirmed its intention to work with local partners to "prevent violent extremism in the United States."*[3] *There is a need, however, to ensure that there is clarity in what one means by the term "violent extremism" and the oft-employed related term of "radicalisation." Equally important, is the imperative to more rigorously lay bare the relationship between these concepts. This article will firstly, attempt the aforementioned task. Second, it will also draw attention to the importance of cognitive extremism as a potential precursor to violent extremism. Third, the article will then identify the key supporting factors that help turn cognitive extremism violent, and finally, the piece will explore possible early warning indicators of the shift from cognitive to violent extremism.*

Radicalisation into Violent Extremism

The argument here is that before one can talk about "violent extremism", one should talk about "radicalisation" first. This is because it should be understood

[1] By Kumar Ramakrishna, Associate Professor and Head, Centre of Excellence for National Security, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. Email: iskumar@ntu.edu.sg. This is a personal comment.

[2] Jamie Bartlett, Jonathan Birdwell, and Michael King. *The Edge of Violence: A Radical Approach to Extremism* (London: Demos, 2010), p. 57.

[3] *Empowering Local Partners to Prevent Violent Extremism in the United States* (Washington D.C.: White House, August 2011).

that while violent extremism is an *outcome or end-state*, radicalisation is best understood as the*process* leading to that outcome. It is fair to say that there has been much discussion in the wider literature about what radicalisation entails, and many understandings implicitly recognise that extremism is integrally related to radicalisation. For example the term "violent radicalisation" has been said to mean the process of adopting or promoting an extremist belief system for the purpose of facilitating ideologically based violence to advance political, religious, or social change.[4] Another popular definition holds that radicalisation entails "the process of adopting an extremist belief system, including the willingness to use, support, or facilitate violence, as a method to effect societal change."[5] The respected terrorism analyst and psychologist John Horgan, on his part, posits that radicalisation refers to the "social and psychological process of incrementally experienced commitment to extremist political or religious ideology."[6] On their part Ciluffo and Saathoff argue that radicalisation "refers to the process by which [individuals] adopt extreme views, including beliefs that violent measures need to be taken for political or religious purposes," and they add that "extreme views" are beliefs that are anti-social, politically rebellious and anti-authoritarian.[7]

Cilluffo and Saathoff, in addition. make a useful analytical distinction between *individual* and *organised* radicalisation. They opine that individual radicalisation results from exposure to an online source or charismatic person espousing extremist ideas. This type of individual may decide to pursue violence on his own, becoming a "lone-wolf" terrorist. He would not necessarily have the support of a network, but may seek out a network in the future, and may be at risk for recruitment at some later date. In fact the mass casualties inflicted by individuals such as Anders Breivik in Norway in July 2011 and Major Nidal Hassan in Fort Hood, Texas in November 2009 underscore the apparent emerging importance of the individual radicalisation pathway and the lone-wolf phenomenon.[8]

[4] "The Violent Radicalisation and Homegrown Terrorism Prevention Act 2007", US Congress.

[5] Charles E. Allen Assistant Secretary for Intelligence and Analysis , Chief Intelligence Officer
Department of Homeland Security 14 March 2007.

[6] Kate Barelle, "Leaving Violent Extremism," presentation at workshop on "Countering Violent Extremism," organised by SEARCCT, Petaling Jaya, Malaysia, 28 August 2012.

[7] Frank Cilluffo and Gregory Saathoff, *Out of the Shadows: Getting Ahead of Prisoner Radicalisation* (Washington D.C. and Charlottesville: The George Washington University Homeland Security Policy Institute and the University of Virginia Critical Incident Analysis Group, 2007).

Cilluffo and Saathoff also point out that organised radicalisation is a process supported by external groups who seek to influence vulnerable individuals. These groups provide psychologically vulnerable individuals with reading materials that promote extremist interpretations of religious or other texts. Individuals are also directed to supportive groups that espouse violence. Organised radicalisation is a relatively structured process then, of "top-down recruiting."[9] These "enabling groups," to employ terrorism scholar Louise Richardson's pithy term,[10] identify individuals with valuable skills who can be recruited to carry out specific actions in support of the group's agenda.[11] Meanwhile in a well-known September 2007 study, the New York Police Department's Intelligence Division forthrightly assert that "terrorism is the ultimate consequence of the radicalisation process." The authors of the study, Mitchell Silber and Arvind Bhatt suggest that in radicalisation, individuals gradually adopt an extremist religious/political ideology which legitimises terrorism as a tool to effect societal change. Moreover, they make the observation that this ideology is continually nourished with a variety of extremist influences. In what represents one of the clearest articulations of the innate links between the concepts of radicalisation and extremism, they argue that "internalising this extreme belief system as one's own is radicalisation." They go on to suggest memorably that the "progression of searching, finding, adopting, nurturing, and developing this extreme belief system to the point where it acts as a catalyst for a terrorist act defines the process of radicalisation."[12] Silber and Bhatt identify four stages of the development of the radicalisation process into violent extremism.[13] In *Pre-Radicalisation*, nothing really remarkable is evident. In *Self-Identification*, they argue that a "cognitive opening" caused by some personal, socio-economic or political crisis increases the chances of radicalisation taking hold in the individual. *Indoctrination* then follows via gradual intensification of extremist beliefs and contact with a "spiritual sanctioner" and a small group of "like-minded"

[8] Ibid.

[9] Ibid.

[10] Louise Richardson, *What Terrorists Want: Understanding the Terrorist Threat* (London: John Murray, 2006), p. 59.

[11] Cilluffo and Saathoff, *Out of the Shadows*.

[12] Mitchell D. Silber and Arvin Bhatt, *Radicalisation in the West: The Homegrown Threat* (New York: NYPD Intelligence Division, 2007). Hereafter NYPD Report.

[13] I have slightly modified their model by substituting the term "violent extremism" for "jihadism." This is because it should be recognised that the radicalisation into violent extremism is not unique to Islamists.

individuals. The final stage could be said to be *Violent Extremism*, where the individual see himself as a fighter ready to engage in violent action.[14] The authors it should be noted are careful to point out that they are not suggesting a simplistic linear progression through each stage into violent extremism. They assert that the reality can be more complex.[15]

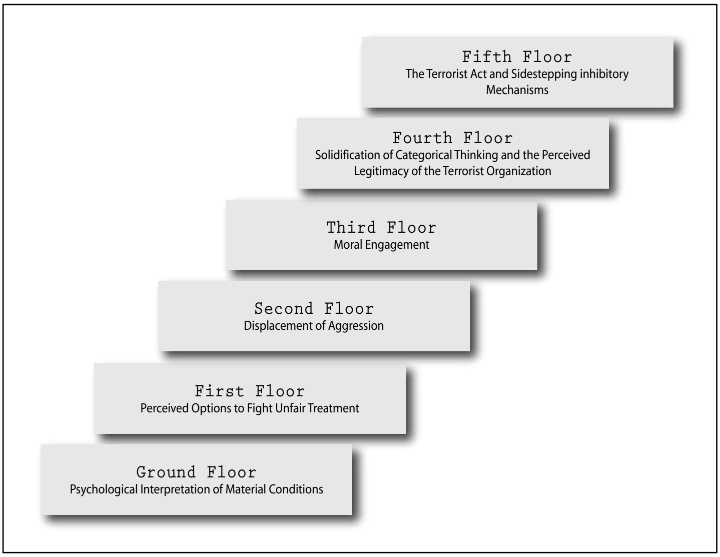
Fifth Floor
The Terrorist Act and Sidestepping inhibitory Mechanisms
Fourth Floor
Solidification of Categorical Thinking and the Perceived Legitimacy of the Terrorist Organization
Third Floor
Moral Engagement
Second Floor
Displacement of Aggression
First Floor
Perceived Options to Fight Unfair Treatment
Ground Floor
Psychological Interpretation of Material Conditions

Figure 1: Moghaddam's Staircase to Terrorism

There are other "stage models" of the radicalisation process into violent extremism. The above figure is from Moghaddam. In this so-called "staircase" concept, the process of radicalisation into violent extremism starts from a situation where an individual, unable to alleviate a perceived adversity, undergoes profound frustration, develops aggressive sentiments that are displaced onto a target group, joins a terrorist organisation and embraces its us-versus-them ideological paradigm, ultimately crossing the moral threshold into out-group violence.[16]

[14] NYPD Report 2007.

[15] NYPD Report 2007.

[16] Fathali M. Moghaddam, *From the Terrorist' Point of View: What they Experience and Why They Come to Destroy* (Wesport and London: Praeger Security International, 2006).

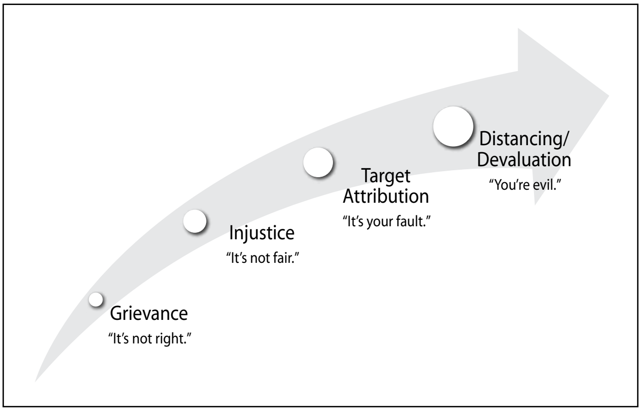

Figure 2: Borum's Four-Stage Model of the Terrorist Mindset

Randy Borum for his part suggests yet another Four-Stage Model of the Terrorist Mindset, in which an individual first frames a particular event, condition, or grievance ("it's not right") as being unjust ("it's not fair"). The radicalising individual then attributes the unjust situation to a target policy, person or nation ("it's your fault"), and ultimately dehumanises that responsible party ("you're evil"). This, Borum suggests, leads to "justification or impetus for aggression."[17]

Apart from stage models there also exist so-called *process models* of radicalisation into violent extremism. The Radical Pathways (RP) Framework, developed by the current author, in contrast to the preceding models by Silber and Bhatt, Borum and Moghaddam is a process model rather than a stage model. That is, rather than seeking to identify particular phases or stages that an individual is likely to pass through in the process of becoming violently radicalised, the RP Framework seeks to lay bare the various factors that may contribute to the individual's so-called "radical pathway." This model suggests a multi-dimensional explanation, arguing that the individual's unique personality characteristics; his immediate social group context; the way that group's ideological frame interprets historical and geopolitical events and forces in ways that call for violent action; cultural

[17] Randy Borum, "Radicalisation into Violent Extremism II: A Review of Conceptual Models and Empirical Research," *Journal of Strategic Security*, Vol. 4, Issue 4 (2011), pp. 38-9.

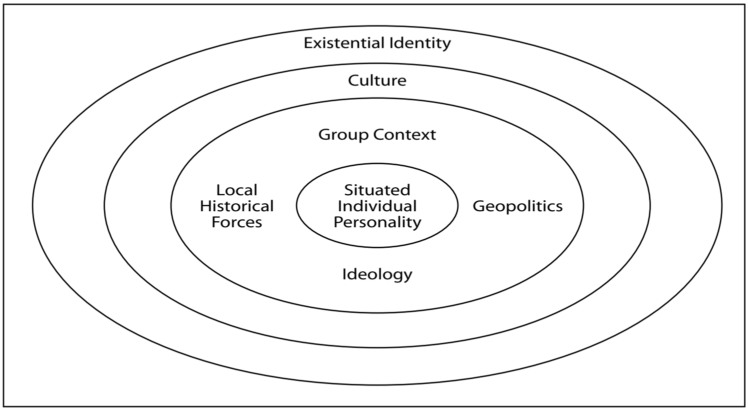

Figure 3: The Radical Pathways (RP) Framework

factors and the universal human drive for a secure and prestigious group identity, all interact in highly idiosyncratic and personalised ways that differ between individuals, to produce various degrees of radicalisation into violent militancy.[18]

Some Caveats

There are, it should be understood, three key problems associated with the use of the term "radicalisation." First, as Borum correctly observes, there has been to date "little discussion and even less consensus" about what "radicalism" means.[19] Second, to be "radical" may mean to reject the status quo in a profound manner, but this does not necessarily entail a rejection expressed in violence.[20] Second, if one looks at the historical record it does seem clear that groups inspired by anti-status quo and hence "radical" ideas in fact generated overall positive outcomes for the wider society. Hence "radical groups" should not automatically be assumed to be socially or politically dangerous and in need of elimination.[21] In fact, a recent review by Robin

[18] Kumar Ramakrishna, *Radical Pathways: Understanding Muslim Radicalisation in Indonesia* (Westport and London: Praeger Security International, 2009).

[19] Randy Borum, ""Radicalisation into Violent Extremism I: A Review of Social Science Theories, *Journal of Strategic Security*, Vol. 4, Issue 4 (2011), p. 9.

[20] Borum, "Radicalisation into Violent Extremism I," p. 9; Bartlett, Birdwell and King, *Edge of Violence*, p. 7.

[21] Cass R. Sunstein, *Going to Extremes: How Like Minds Unite and Divide* (New York: Oxford University Press, 2009), p.149.

L. Thompson of a recent book by social psychologists Clark McCauley and Sophia Moskalenko, correctly avers that at times "radicalisation is good and radicalised persons motivate others to take action for the good of humanity."[22]

Such caveats apply to the term *violent extremism*, like "radicalisation" equally widely used in current scholarly and policy discourse. At its most basic, extremism suggests "being at the margins, of existing on the boundaries or of functioning at the edges," and only tenuously linked to the normative core or centre.[23] "Extremism," Douglas Pratt informs us, "takes its own wider group identity – be it religion or tradition – to an extreme; not by a move away from the centre, but rather by intensifying its self-understanding and self-proclamation as representing, or being, the centre;" hence extremism represents a significant heterodoxy as opposed to normative orthodoxy.[24] Extremism, by definition, the eminent Australian scholar Greg Barton reminds us, involves rejecting the mainstream for the "extraordinary and the atypical." It can also mean "rejecting the moderate and balanced for the uncompromisingly 'pure' – and rejecting shades of grey for black and white."[25] It has been suggested that many of the same problems afflicting the use of the term *radicalisation* apply to the word *extremism* as well: there is little consensus on what the term means; being extremist in one's views does not necessarily mean being violent; while as the incisive political scientist Cass Sunstein pointedly observes, when "people shift from indifference to intense concern with local problems, such as poverty and crime," then "extreme movements are good, even great."[26]

It is, nonetheless, widely recognised by terrorism scholars and practitioners everywhere that the phenomenon of radicalisation into violent extremism is an all-too-real and dangerous phenomenon. Some scholars have, in this regard, even recently coined a new term Radicalisation and

[22] Robin L. Thompson, review of Clark McCauley and Sophia Moskalenko, *Friction: How Radicalisation Happens to Them and Us* (New York: Oxford University Press, 2011), Journal of Strategic Security, Vol. 4, Issue 4 (2011), pp. 195-6.

[23] Douglas Pratt, "Religion and Terrorism: Christian Fundamentalism and Extremism," *Terrorism and Political Violence*, Vol. 22, No. 3 (July 2010), p. 440.

[24] Pratt, "Religion and Terrorism," p. 440.

[25] Greg Barton, "Identity, Violent Extremism, and Strategic Communication in the Digital Age," presentation at workshop on "Cyberia: Identity, Cyberspace, and National Security," organised by The Asia Pacific Center for Security Studies (APCSS), Singapore, 22 August 2012.

[26] Borum, "Radicalisation into Violent Extremism I," p. 9; Sunstein, *Going to Extremes*, p. 149.

Involvement in Violent Extremism (RIVE).[27] To be sure, violent extremism manifests in many forms. As discussed, one such form is organised terrorism, such as the September 11 2001 Al Qaeda strikes in New York and Washington D.C. and the Bali bombings by Jemaah Islamiyah in October 2002. There is also as mentioned, individual or "lone-wolf terrorism," as exemplified by Timothy McVeigh in the April 1995 bombing of the Murrah Building in Oklahoma City; the Fort Hood shootings by Major Nidal Hassan in November 2009; and more recently the Norway attacks by Anders Breivik in July 2011. It should also be recognised, though, that violent extremism also drives other forms of out-group violence such as the inter-group ethnic or religious violence that tore the Balkan states asunder between 1992 and 1995;[28] as well as the horrific Hutu-Tutsi violence in Rwanda in 1994.[29]

Cognitive and Violent Extremism: Recent Thinking

In a recent essay, the American analyst, Lorenzo Vidino, makes the critical observation that while the threat of violent radicalism needs addressing, equally important to note is that "cognitive radicalism" should not be overlooked either. This is because cognitive radicalism is "widely understood to be the logical antecedent to behavioral radicalism."[30] In line with this logic, for our purposes we may assert that *cognitive extremism* exists when an individual immoderately refutes the legitimacy of the existing social order and seeks to replace it with a new structure based on a completely different belief system. *Violent extremism* then happens when an individual takes the additional step of using violence to further the views derived from cognitive extremism.[31]

To be more precise, *cognitive radicalisation leads to cognitive extremism.* Cognitive radicalisation can be thought of as a *drastic identity simplification*

[27] Sara Savage, "Four Lessons from the Study of Fundamentalism and Psychology of Religion," *Journal of Strategic Security*, Vol. 4, Issue 4 (2011), pp. 131-150.

[28] Michael Ignatieff, *The Warrior's Honor: Ethnic War and the Modern Conscience* (New York: Owl Books, 1997).

[29] Neil J. Kressel, *Mass Hate: The Global Rise of Genocide and Terror*. Rev. and updated ed. (Cambridge, MA: Westview Press, 2002), pp. 73-100.

[30] Lorenzo Vidino, *Countering Radicalisation in America: Lessons from Europe* (Washington D.C: United States Institute of Peace Special Report 262, November 2010), pp. 4-5.

[31] Ibid., p. 4.

dynamic. This requires elaboration. In general, as the Nobel laureate Amartya Sen memorably puts it:

> *"The same person can, for example, be a British citizen, of Malaysian origin, with Chinese racial characteristics, a stockbroker, a nonvegetarian, an asthmatic, a linguist, a bodybuilder, a poet, an opponent of abortion, a bird-watcher, an astrologer, and one who believes that God created Darwin to test the gullible".*[32]

However, when the members of a social group perceive that they collectively face the threat of either direct physical or more profoundly, cultural extinction at the hands of a powerful adversarial "Them," all these diverse social identities get drastically honed down to *one single dimension or axis of collective identification that is perceived to be at risk*. Slavenka Drakulic, in this respect, well describes the cognitively radicalising impact on the Croat population of Serb attacks during the Balkan wars of the early 1990s:[33]

> *"Along with millions of other Croats, I was pinned to the wall of nationhood – not only by outside pressure from Serbia and the Federal Army but by national homogenisation within Croatia itself. That is what the war is doing to us, reducing us to one dimension: the Nation. The trouble with this nationhood, however, is that whereas before, I was defined by my education, my job, my ideas, my character – and yes, my nationality too - now I feel stripped of all that (emphasis mine)".*

A similar observation was articulated by Lord Alderdice, the trained psychiatrist and perceptive politician who played a leading role in brokering the Good Friday agreement between Catholic and Protestant factions in Northern Ireland in April 1998. He pointed out that during the Troubles in Northern Ireland, "the community had regressed" – or undergone a drastic identity simplification dynamic – "from a myriad of individual differences maintained in a broad mosaic of relationships, to a narrower frame of reference where *the single difference between Protestant Unionist and Catholic Nationalist*

[32] Amartya Sen, *Identity and Violence: The Illusion of Destiny* (London: Allen Lane, 2006).
[33] See Ramakrishna, *Radical Pathways*, p. 34.

assumed pre-eminence (emphasis mine)"[34] *In our terms, both communities in Ulster had undergone a process of cognitive radicalisation into a more or less collective state of cognitive extremism.* That is, the multiple identities within one community had been drastically simplified to a single overarching in-group: "Us," while the multiple affiliations and self-identifications in the other community were similarly reduced to a single overarching, adversarial "Them," the out-group. Hence, whether we are talking about Irish Catholics and Protestants in Ulster; Serbs, Croats and Bosnian Muslims in rapidly dissolving Yugoslavia, Tamils and Sinhalese in conflict-torn Sri Lanka; Shia and Sunni in post-Saddam Iraq and Christians and Muslims in conflict-prone eastern Indonesia, what ties them together despite their different circumstances and bases of identity is the fact that *these were all cognitively radicalised communities*. Communities, like individuals, can cognitively radicalise as well.[35] In this connection it is telling that a recent report by the Washington Institute for Near East Policy points out that violent extremist ideologues "in nearly all cases," take pains to "suggest that many aspects of a person's identity can be - indeed must be - reduced to being 'Muslim,' to the exclusion of other identities."[36] The upshot of this discussion is simple. Such *drastic intra- and inter-group identity simplification* - the true essence of the cognitive radicalisation process – must occur long before any extremist belief system justifying out-group violence is consciously adopted and for that matter, resorted to in the real world.

The mindset of the cognitive extremist towards his respective ethnic, nationalist or religious out-group is not a particularly salubrious one. James Waller puts it pithily:

> *"Our cause is sacred, theirs is evil.*
> *We are righteous; they are wicked.*
> *We are innocent, they are guilty.*
> *We are the victims, they are the victimisers"*[37]

[34] Alderdice cited in Ramakrishna, *Radical Pathways*, pp. 33-4.

[35] Thompson, review of McCauley and Moskalenko, *Friction*, p. 195. McCauley and Moskalenko highlight the reality of "mass radicalisation."

[36] J. Scott Carpenter, Matthew Levitt, Steven Simon, and Juan Zarate, *Fighting the Ideological Battle: The Missing Link in US Strategy to Counter Violent Extremism* (Washington DC: Washington Institute for Near East Policy Strategic Report, 2010), p. 8.

[37] James Waller, *Becoming Evil: How Ordinary People Commit Genocide and Mass Killing* (New York: Oxford University Press, 2005), p. 243.

If history teaches us anything, it is that it is very dangerous when the out-group begins to be seen as evil, immoral, sub-human and linguistically dehumanised. Linguistic dehumanisation of the out-group often results in their *social death* – or exclusion from the well-defined and ardently defended moral circle of in-group members.[38] It is telling in this respect, that during the Rwandan genocide, Hutu extremists called the Tutsi rivals *inyenzi* – meaning "cockroaches" or "insects;" while Nazis euphemistically redefined Jews as *inter alia*, "parasites," "filth," "excrement," "plague", or "tuberculosis."[39] Haig Bosmajian correctly warns that the "distance between the linguistic dehumanisation of a people and their actual suppression and extermination is not that great."[40] Linguistic dehumanisation in the religious sphere has arguably even more dire implications: if the out-group is cognitively reconstrued and linguistically portrayed as evil beings, then a process of *satanisation* takes hold. Under such circumstances, out-group enemies deemed to "embody pure evil," religious scholar and psychoanalyst James W. Jones tells us, "cannot be argued with or compromised with; they can only be destroyed," as a "moral duty."[41]

It is arguably from such wider cultures of hatred,[42] or cultures of violence[43] comprising *cognitively extremist haters* of varying degrees of intensity, that the smaller minority of dangerous *violent extremist killers* emerges. This, however, is by no means a linear, deterministic process. It has been increasingly recognised, nevertheless, that "violent potentials" do exist within cognitive extremism, including religiously-driven cognitive extremism.[44] However, the transition from cognitive to violent extremism requires the intervention of four sets of supporting factors: culture, ideology, small-group dynamics and an enabling environment.

[38] Ibid., pp. 236-7.

[39] Ibid., p. 246.

[40] Ibid.

[41] James W. Jones, *Blood that Cries out from the Earth: the Psychology of Religious Terrorism* (Oxford: Oxford University Press, 2008), p. 44.

[42] Willard Gaylin, *Hatred: The Psychological Descent into Violence* (New York: Public Affairs, 2003), p. 195.

[43] Mark Juergensmeyer, *Terror in the Mind of God: The Global Rise of Religious Violence*, updated ed. with a new preface (Berkeley and Los Angeles: University of California Press, 2000), pp. 10-15

[44] Charles B. Strozier, David M. Terman, and James W. Jones, with Katharine A. Boyd , eds., *The Fundamentalist Mindset: Psychological Perspectives on Religion, Violence and History*, (Oxford and New York: Oxford University Press, 2010), Strozier et al. (2010).

Supporting Factors in the Transition from Cognitive to Violent Extremism

Culture

The eminent Dutch social psychologist Geert Hofstede, following a massive study of 74 countries worldwide, identified, *inter alia*, three dimensions of national cultures[45] that are particularly pertinent for our purposes: "*collectivism versus individualism," power distance* (from small to large)" and *uncertainty avoidance* (from weak to strong.)"[46] First, collectivism refers to the organising principle of societies in which "people from birth onward are integrated into strong, cohesive in-groups, which throughout people's lifetimes continue to protect them in exchange for unquestioning loyalty."[47] Second, power distance is the extent to which the less powerful members within a social collective "expect and accept that power is distributed unequally."[48] Finally, uncertainty avoidance is "the extent to which the members of a culture feel threatened by ambiguous or unknown situations" and search for solace in larger collectives that offer them existential certainty.[49] In collectivist societies, personal opinions are subordinated to the collective will of the group and its senior elders.[50] Collectivist societies also tend to be large power-distance societies in which the lower classes depend on the power elites for preserving social security and harmony; respect for parents and older relatives is a lifelong basic virtue; and teachers are deeply revered.[51]

Finally in strong uncertainty-avoidance societies – that is, societies which are relatively uncomfortable with uncertainty and ambiguity - children are socialised into firm rules of what is dirty and taboo; school students seek "the right answers" which teachers are expected to have; and society as a

[45] There are many academic definitions of the term "culture." One useful way of thinking about culture is those learned "patterns" of thinking, feeling and potentially acting. Such patterns distinguish one social group from another. See Geert Hofstede and Gert Jan Hofstede, *Cultures and Organisations: Software of the Mind: Intercultural Cooperation and its Importance for Survival*, rev. and expanded 2nd edn. (New York: McGraw-Hill, 2005), pp. 2-4, 377.

[46] Hofstede and Hofstede, *Cultures and Organizations*, p. 23.

[47] Hofstede and Hofstede, *Cultures and Organizations*, p. 76.

[48] Hofstede and Hofstede, *Cultures and Organizations*, p. 46.

[49] Hofstede and Hofstede, *Cultures and Organizations*, p. 167.

[50] Hofstede and Hofstede, *Cultures and Organizations*, pp. 75-114.

[51] Hofstede and Hofstede, *Cultures and Organizations*, pp. 51-72.

whole prefers numerous, precise rules for regulating social behavior. In fact, there is an emotional need for rules and regulations.[52] Hofstede observes that strong uncertainty-avoidance cultures tend to evince greater levels of xenophobia and ethnic prejudice, and in particular, the conviction that in religion, there "is only one Truth and we have it."[53] Hence it is largely the strong uncertainty-avoidance cultures that tend to develop "religious, political, and ideological intolerance and fundamentalisms."[54] Hofstede concludes that countries with diverse "ethnic, linguistic, or religious groups" whose respective cultural outlooks are characterised by *collectivism* and *strong uncertainty avoidance* are especially vulnerable to "violent intergroup strife."[55]

Ideology

Culture is best understood as the "unwritten rules of the social game."[56] Culture by itself is insufficient to mobilise social groups for action. This is why Willard Gaylin argues that "calculated propaganda" is required to "mobilise the population."[57] This is where ideology comes into the picture. C.J.M. Drake defines ideology to mean those "beliefs, values, principles and objectives" by which a group "defines itself and justifies its course of action."[58] While to be effective, ideology must certainly draw upon and well known if inchoate and free-floating cultural symbols, stories, and themes, it is more deliberately held and action-oriented than culture. While culture as noted is unwritten and shared largely without mass conscious awareness, ideology is primarily a relatively well articulated set of beliefs and ideas that are consciously held to varying degrees by members of a group, and that provide an agenda for action.[59] It is not for nothing that the respected terrorism

[52] Hofstede and Hofstede, *Cultures and Organizations*, pp. 163-89.
[53] Hofstede and Hofstede, *Cultures and Organizations*, pp. 198-99.
[54] Hofstede and Hofstede, *Cultures and Organizations*, pp. 197-202.
[55] Hofstede and Hofstede, *Cultures and Organizations*, pp. 196-7.
[56] Hofstede and Hofstede, *Cultures and Organizations*, p. 4.
[57] Gaylin, *Hatred*, p. 178.
[58] C.J.M. Drake,"The Role of Ideology in Terrorists' Target Selection, *Terrorism and Political Violence*, Vol. 10, No. 2 (Summer 1998), pp. 53-85.
[59] Waller, *Becoming Evil*, p. 183.

scholar Louise Richardson points out that a "legitimising ideology" is part of the "lethal cocktail" that generates terrorist action.[60]

Small-Group Dynamics

In fact, as mentioned earlier, Richardson opines that ideology aside, an "enabling group" is also part of the mix of factors supporting the transition to out-group violence.[61] This is especially so in the case of a small group – real-world or even on-line – that is largely insulated from outside influences, and is, for all intents and purposes, not unlike a *religious cult*. The cult specialist Arthur Deikman observes that a religious cult evinces total dependence on a leader; utter compliance with the group; suppression of dissent; and finally and of no small importance, devaluation of outsiders.[62] It is hence within the small cult-like group that the free-floating prejudices of the *wider culture of cognitive extremism* are intensified and focused into a relatively coherent and more or less consciously held violent ideology - and *cognitive extremism arrives at the very cusp of out-group violence*.

Enabling Environment

All that remains then for cognitive extremism to tip over into violence is for an enabling environment to obtain: that is, a situation in which objective social, economic and political grievances that empower and fuel violent extremist ideology, dangerously meshes with systemic governmental corruption, weak counter-extremism capacities and regulatory controls, and ultimately ease of access to weapons material and expertise.

[60] Richardson, *What Terrorists Want*, p. 59.
[61] Richardson, *What Terrorists Want*, p. 59.
[62] Arthur J. Deikman, *Them and Us: Cult Thinking and the Terrorist Threat*. Berkeley: Bay Tree Publishing, 2003), p. 52.

Early Warning Indicators of the Transition from Cognitive to Violent Extremism

A final question worth asking is how would we know that the transition from cognitive to violent extremism is imminent? Are there "early warning indicators" of such a transition, so to speak? In recent years analysts have begun addressing this issue. The American analysts Daveed Gartenstein-Ross and Laura Grossman, based on a study of 117 violent Islamists in the US and UK, identified six common indicators of the process of radicalisation into violent extremism of these individuals: first, a legalistic interpretation of Islam; second, trusting the interpretations of a "select and ideologically rigid set of religious authorities;" third, perceiving an "inherent schism between Islam and the West;" fourth, displaying a low tolerance of "perceived theological deviance," even violently opposing "alternative interpretations and practices"; fifth, imposing their preferred religious interpretations on others; and ultimately, observably adopting the view that the only proper response is "military action."[63] More recently, the Australian analysts Mark R. Kebble and Louise Porter, building upon the Silber/Bhatt stage model of radicalisation discussed earlier reckon that the transition to out-group violence is likely when certain risk factors are present. These include "beliefs by violent extremists that they are retaliating;" that "potential victims are less than human;" and that "their actions are religiously justified." Additional risk factors include social isolation from "positive influences;" a demonstrated "capability for violence," and a predilection to "access violent materials."[64]

Closing Reflections

In this article we have sought to introduce clarity into the discussion of the oft-used terminology of "violent extremism" and "radicalisation," as well as more rigorously tease out the symbiotic conceptual relationship between these ideas. In the process we explored stage and process models

[63] Daveed Gartenstein-Ross and Laura Grossman, *Homegrown Terrorists in the US and UK* (Washington D.C: Foundation for Defense of Democracies Press, April 2009), pp. 12-13.

[64] Mark R. Kebbell and Louise Porter, "An Intelligence Assessment Framework for Identifying Individuals at Risk of Committing Violent Extremism against the West," *Security Journal*, Vol. 25, No. 2, pp. 212-28.

of radicalisation into violent extremism and seen that while “radicalisation” is a process, “extremism” is the outcome of that process. After discussing some caveats regarding radicalism and extremism, the article also offered fresh thinking on how cognitive extremism could be regarded as a potential precursor to violent extremism. In this respect, we saw how a drastic identity simplification dynamic is the real key to understanding cognitive radicalisation. This was followed by a discussion of how culture, ideology, small-group dynamics and an enabling environment all play roles as key supporting factors that help turn cognitive extremism violent. Finally, the piece explored possible early warning indicators of the shift from cognitive to violent extremism. The ideas discussed here are not intended to be seen as the definitive views on the subject at hand. Rather, it is hoped that they will stimulate further discussion in both analytical and practitioner circles about radicalisation into violent extremism – a continuing and complex challenge facing our simultaneously globalised and yet fragmented world.

BATTENING DOWN THE HATCHES: SOME REFLECTIONS ON PROTECTING THE MARITIME SUPPLY CHAIN FROM MARITIME TERRORISM

Nazery Khalid[1]

"He shall spurn fate, scorn death, and bear his hopes 'bove wisdom,
grace and fear.
And you all know, security is mortals' chiefest enemy"
(William, Shakespeare : 'Macbeth')

A changed world for the worst?

The importance of the seas in facilitating global trade and economic prosperity cannot be overemphasised. An estimated 85% of world trade is carried by seaborne transport[2] and offshore oil and gas contributes to around 70% of global oil and gas supplies.[3] People around the world depend on various maritime economic activities such as fishery and marine tourism, and along coastal areas, for their livelihood and many of them live in coastal areas. Naval forces count on freedom of the sea in the global commons to enable their movements and safeguard their nations' strategic interests.

It would, therefore, not be an exaggeration to say that without security at sea, many of these activities would be interrupted or even halted. Should there be any untoward incident at sea that causes shipping traffic to be interrupted or economic activities such as offshore oil and gas exploration and production to be impeded, there would be serious repercussion to global trade and economy. In addition, the strategic interests of the state bordering the seas and the international community that depends on the uninterrupted movement of ships in the sea would be compromised. The impact of piracy in the Gulf of Aden, a key shipping lane especially for energy transport, on shipping companies, shippers and global trade underlines the importance of protecting such a sealane from security threats.

[1] Senior Fellow, Maritime Institute of Malaysia (MIMA). The opinions expressed are the author's own.
[2] UNCTAD (2011). Review of Maritime Transport. Geneva : UNCTAD.
[3] Estimate by Oil and Gas International (OGI), the leading online source of the oil and gas industry data and information, in 2010.

As a measure of how much the world has changed since the September 11, or '9/11' attacks, concerns over security have gripped the attention of policymakers and the public. Amidst the dramatically changed, and still changing, post 9/11 landscape, the maritime sector has also undergone tremendous changes from a security perspective. This underscores concerns of the vulnerability faced by seaborne transport, lives, and assets in the maritime sector to the threat of terror.

While measures undertaken to boost security along the maritime supply chain[4] have added a sense of security to players along the maritime supply chain, those in charge of security should not be complacent. New, asymmetrical and non-conventional threats are always evolving. Terrorists are always thinking of new and innovative ways to strike.

The last decade or so has seen a range of transport modes being targeted; namely aviation (commercial airplane strikes during 9/11; attacks on airports in Moscow in 2011, Glasgow in 2007 and Brussels in 1979), road (bus bombing in London in 2005 and various attacks on buses in Israel), rail (train bombings in London in 2005 and Madrid in 2004). These attacks underscore the 'attractiveness' of these targets to terrorists who are hell-bent on causing as much damage and as many deaths as possible.

The Bane of Maritime Terrorism

Since the 9/11 attacks, a considerable amount of literature has emerged on the subject of 'maritime terrorism'. The Council for Security Cooperation in the Asia Pacific (CSCAP) Working Group has come up with an arguably useful and reasonable definition for 'maritime terrorism' as follows :

"…the undertaking of terrorist acts and activities within the maritime environment, using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities"

[4] In the context of this paper, 'maritime supply chain' refers to the network that links producers and consumers that includes a maritime transportation component and consists of maritime-related assets such as ships and ports.

Meanwhile, Jane's Intelligence Review defines 'maritime terrorism' as:[5]

"…the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change, in the maritime domain".

Burns (2004) defined 'maritime terrorism' as:[6]

"… terrorist acts executed within, or with the intent of compromising the features of the maritime domain".

Terrorists are driven by ideological and political motives.[7] They operate in fairly well organised groups[8]; among the more well-known ones are Abu Sayyaf which claimed responsibility for the Superferry 14 bombing and Al-Qaeda which claimed credit for the USS Cole and Limburg attacks, have some form of training and deploy fairly sophisticated tactics in pulling off attacks. They plan their attacks well in advance, complete with sketches, plans and intelligence collection. They tend to have backers who provide financing and the logistics to prepare and mount the attacks. They seek to cause as much damage, shock and destruction as possible and generate maximum publicity to highlight their cause. Unlike pirates, terrorists take no prisoners and are even willing to die in the process of carrying out their deeds.

Among the high-profile attacks on maritime targets in recent times were:[9]

i) The hijacking of the cruise ship *Achille Lauro* in Egyptian waters in 1985 which claimed the life of a disabled passenger;

[5] See 'Drawing the Line between Piracy and Maritime Terrorism', *Jane's Intelligence Review*, September 2004, 3.

[6] See Burns, R. H. (2004). 'Terrorism in the Early 21st Century: Maritime Domain', *IDSS Maritime Security Conference*, 20–21 May 2004. See also Hoffman, B. (2003). Inside terrorism, New York : Columbia University Press. He defined terrorism as "deliberate creation and deliberation of fear through violence or the threat of violence in the pursuit of political change"

[7] In this regard, the definition offered by Hoffman (2003) is instructive. He described terrorism as "deliberate creation and deliberation of fear through violence or the threat of violence in the pursuit of political change". See Hoffman, B. (2003). Inside terrorism, New York : Columbia University Press.

[8] See Richardson, M (2004).

[9] For a reference of chronicles of terrorist/criminal activities aimed at maritime targets, see among others Shie, T. R. (2005) 'The Nexus between Counterterrorism, Counterproliferation and Maritime Security in Southeast Asia', *CSIS Issues & Insights*, 4(4), 2005, available at <http://www.csis.org/pacfor/issues/v04n04_ch3.cfm>. See also Burns, R. H. (2004).

ii) The attack on the United States Navy ship, *USS Cole* by an explosive-laden speedboat in the waters off South Yemen in 2000;
iii) The attack on *Our Lady of Mediatrix* in the waters off Manila in 2000;
iv) The kidnapping of 21 people (including 10 foreign tourists) from Sipadan Island, a popular diving spot off Sabah, in 2002 by Abu Sayyaf Group;
v) The attack on the French tanker *Limburg* by an explosive-laden speedboat in the waters off South Yemen in 2002 which killed a crew member of the tanker;
vi) The bombing and sinking of the passenger vessel *Superferry 14* in 2004 in the waters near Manila killing 116 passengers (this to date remains the world's deadliest maritime terror attack); and
vii) The suicide bombing attack on the Port of Ashdod in Israel in 2004 which killed 16 people including the bombers.

Tragic and unfortunate as those attacks were, they provided valuable lessons and useful references for security agencies, regulatory authorities and players along the maritime supply chain to help develop a better understanding of the risks and threats of maritime security and to prepare the necessary resources and responses to mitigate them. Analysing the factors and circumstances involved in those attacks would enable the authorities and security agencies to sketch the typology of maritime terrorism. This will help them to identify the potential threats and possible means and targets in order to propose effective countermeasures.[10]

Given the stealth, unpredictable and sometimes sophisticated nature of these terrorist groups, there is a need for security agencies, policymakers and players along the supply chain to understand the features and workings of the maritime supply chain. This is important to enable the right resources to be allocated, the appropriate skills to be developed and the necessary hardware (equipment, systems) to be installed to anticipate, thwart or respond effectively to threats of terror. This is important, given that the maritime

[10] Terrorist attacks on maritime targets may not just be direct assaults on vessels and ports, as have been recorded, but may include scuttling of vessels, smuggling of weapons and terrorists in containers, and jamming of systems at ports to sabotage operations and cause disruption to the supply chain. Some of these scenarios were discussed in various literature, for example in Burns, R. H. (2004) and Raman, B. (2004), 'Maritime Terrorism: An Indian Perspective', *International Conference on National Security in a Changing Region held in Singapore*, 28–29 October 2004.

realm provides a vast theater for terrorists to operate. Terror groups have been known to have the propensity to target high-value maritime interests beyond what they have already attacked.[11]

Protecting the Maritime Supply Chain

Post 9/11, there have been a slew of maritime security measures introduced to boost the security of lives and assets at sea and onshore. They include:

i) Container Security Initiative (CSI), an initiative by the US Customs and Border Protection (CBP) Unit under the Department of Homeland Security, CSI is based on four principles, namely using intelligence and automated information to identify and target containers that pose a risk for terrorism, pre-screening those containers that pose a risk at the port of departure before they arrive at US ports, using detection technology to quickly pre-screen containers that pose a risk, and using smarter, tamper-evident containers

ii) Customs Trade Partnership Against Terrorism(C-TPAT), an initiative of the US CBP under which shippers commit to improving the security of their cargo shipments, and in return, receive a variety of benefits from the US Government such as the pre-clearance of cargoes.

iii) The International Ship and Port Facility Security Code (ISPS Code), a comprehensive set of measures introduced by IMO in 2002 to enhance the security of ships and port facilities. It was introduced in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks.

[11] It was revealed that Al Qaeda had its own network of ships and agents and had developed a sort of manual to carry out attacks on maritime targets. The manual came with instructions on how to use mines and turn LNG tankers into floating bombs. An Al-Qaeda operative believed to be its 'head of naval operations' was captured in November 2002 with a 180-page dossier listing possible maritime targets. See Bingley, B. (2004), 'Security Interests of the Influencing States: The Complexity of Malacca Straits', *The Indonesian Quarterly*, 32(4), 2004, 358.

iv) Megaports Initiative, introduced in 2003 as part of the Second Line of Defence Program of the National Nuclear Security Administration of the US Department of Energy. The initiative focuses on high-risk and high-volume ports based on their attractiveness to smugglers of nuclear materials and weapons, and entails maximum inspection of containers at those ports regardless of their origin and destination.

v) The Proliferation Security Initiative (PSI), introduced by the US Government in 2003 to curb the spread of weapons of mass destruction (WMD) and related materials. PSI provides a platform to coordinate governmental non-proliferation activities globally in the face of advanced communications technologies and expanding global trade that have facilitated the smuggling of WMD.

vi) The Regional Maritime Security Initiative (RMSI), a partnership of willing regional nations with varying capabilities and capacities to identify, monitor, and intercept transnational maritime threats under existing international and domestic laws. This rather controversial initiative empowers participating nations with the timely information and capabilities they need to act against maritime threats in their own territorial seas, and deciding for themselves what response, if any, they need to take.

vii) The Secure Freight Initiative (SFI), an initiative by the US to inspect all containers at high-risk ports through an integrated inspection system with an international shipping company to secure the global supply chain against the threat of terror.

viii) The 24-Hour Rule, an initiative led by the US that requires 24-hour notice before cargo is loaded on vessels. High-risk containers, identified prior to vessel loading, are inspected at the port of origin.

These initiatives have enhanced security along the maritime supply chain. However, there is certainly much room for improvement to boost security along the maritime supply chain to prevent terrorists' strikes there.

The following initiatives which have been identified as requiring attention and strengthening in order to boost security along the maritime supply chain are:

i) Enhancing cooperation among all parties along the maritime supply chain, which is essential in foreseeing and confronting terror attacks. In this regard, partnerships among local authorities and state and federal governments must be promoted and enhanced. This cooperation should include developing contingency and emergency operation plans that enable local, state and federal governments and private entities to work effectively together to coordinate routine and emergency response mechanisms in the face of terror threats. Also, given the transboundary nature of maritime crimes, greater international cooperation must be encouraged to boost maritime security especially in SLOCs and key waterways.

ii) Developing adequate capability to undertake quality counterterrorism intelligence and analysis. In addressing the threat of terror in the wide and complex expanse of the maritime supply chain, the need for accurate, timely and relevant intelligence cannot be overemphasised. Quality intelligence is crucial in enabling the development of risk management solutions that can result in maximum security impact and minimum threat exposure to lives and assets along the maritime supply chain.

iii) Securing critical maritime-related ICT infrastructure and cyberspace. Operations in sectors such as shipping, ports and offshore exploration and production are increasingly sophisticated and facilitated by high-tech equipment and systems. Terrorists may find hacking into these systems and paralysing the equipment an attractive prospect as it does not require too much resources and visibility to carry out but can, nonetheless, create havoc along the maritime supply chain. As such, there must be a solid 'cyberdefence' in place to safeguard critical infrastructure and essential digital systems and technologies in the maritime realm.

iv) Securing maritime checkpoints at ports and passenger terminals by reviewing immigration procedures and addressing loopholes and weak points.

v) Enhancing emergency management; medical evacuation and preparedness; public health management; and search and rescue operations with a view to inculcating a culture of alertness, proactiveness and a readiness to respond to terror threats and attacks at all times.

vi) Inculcating a sense of accountability among all the parties along the maritime supply chain. It is vital to drive home the point that securing the chain from the threat of terror is the responsibility of everyone along it. There is a need to strongly emphasise to concerned parties that they have a collective interest in securing the chain and hence must always alert one another if they suspect, know of or see something amiss or suspicious.

vii) Preventing the flow of financing and support towards terrorists and raiding institutions and arresting individuals promoting radicalism and ideologies that can foment terrorism.

viii) Leveraging the use and application of technology to come up with innovative and cutting-edge solutions to enhance information sharing among parties in the maritime supply chain in combating the threat of maritime terrorism.

ix) Increasing patrols especially in SLOCs and known areas and 'logistical corridors' where terrorists operate, to show presence and to provide a deterrence to them. Joint or coordinated patrols among navies of countries bordering SLOCs should be carried out within a regional cooperation framework to ensure consistency, efficiency and sustainability of the patrols.

x) Sharing of information among littoral nations and among the larger international community that can lead to anticipation of attacks and preparation of adequate and appropriate responses to thwart and counter them.

xi) xi) Not underestimating any potential terror threats to maritime targets. Consider the threat to turn tankers into floating bombs, a scenario imagined by several scholars after the 9/11 attacks, which was dismissed by shipping practitioners who doubted the practicality and effectiveness of doing so. The dismissal of a threat could lead to the lack of vigilance that could come at a high price to lives and assets along the maritime supply chain and beyond, should such attacks materialise.[12] It is also important not to underestimate the possibility of linkages between or among terrorist groups in different locations that may share resources and expertise to mount attacks against maritime terrorists.[13]

xii) Assisting developing nations bordering waters where terrorists are known to operate and most likely to strike, in building their capability and capacity in counter-terrorism. This includes assistance in both the areas of defense (equipment, systems, personnel, institutional framework) and deterrence (legal framework) to prevent terrorism and also to fight and prosecute terrorists.

Getting the Balance Right

Acts of maritime terrorism may be few and far between but the fallout arising from them can be far-reaching and even generate catastrophic impact to the littoral state(s) of the sites of the attacks and to the larger international community. The fact that the impacts of the attacks that have occurred thus far, as listed earlier in this article, were localised or at most regionalised should not allow stakeholders along the maritime supply chain to rest on their laurels.

[12] The revelation in 2004 of a statement allegedly prepared by Al-Qaeda leader Osama bin Laden exposed the terror group's plan to attack Western oil interests. Excerpt from the statement, in reference to the *Limburg* attack in 2002 : "*By exploding the oil tanker in Yemen, the holy warriors hit the umbilical cord and lifeline of the crusader community, reminding the enemy of the heavy cost of blood and the gravity of losses they will pay as a price to their continued aggression on our community and looting of our wealth*". See Burns, R. H. (2004), 8.

[13] It was suggested that LTTE, which was known to have a fairly sophisticated maritime terrorism capability, had links with JI which could have been intended to boost the latter's capability to conduct attacks on maritime targets. See Borgu, A. (2004). 'Maritime Terrorism: An Australian Perspective', *Workshop on Maritime Counter Terrorism of the Observer Research Foundation*, 29–30 November 2004.

We can be encouraged that governments worldwide have upped the ante and paid greater attention to maritime supply chain security since 9/11. However, measures to boost security along it should not come at the expense of attaining a smooth flow of the maritime supply chain which is crucial in facilitating global trade and economic growth. For example, proposals to screen all containers without taking into account their different levels of potential risks, is anathema to efficient movement of cargos along the maritime supply chain.[14] It is unrealistic to check every single container and at the same time expect that it would not have an impact on the smooth flow of the maritime supply chain and add to the cost of transporting goods through the chain.

The cost of securing the maritime supply chain from terrorist threats should not be too prohibitive, especially to developing countries which do not have the financial means or the capability to confront this threat on their own. Developed countries should help developing countries build capacity in areas such as collection of intelligence; identification of existing and potential threats; compliance with international security measures; and the establishment of security plans, policies, procedures and systems. However, the assistance rendered must not come with any pre-conditions and must be in accordance with international principles and laws. Efforts must also be made to ensure that the implementation of measures to counter terrorist threats on the maritime supply chain must not result in the incurrence of costs and inconvenience which cannot be borne, or tolerated by others.

In this regard, the successful countermeasures taken by the littoral states of the Straits of Malacca could be emulated by others fighting maritime terrorism. Their comprehensive approach to maritime security not only involves confronting the threats at sea but also in dismantling the terror network on land and addressing the root causes of terrorism. A piecemeal approach to securing the maritime supply chain would not do, given the extent of the chain; the many players, assets, processes and systems involved; and the huge volumes and variety of cargos passing through it. Equally important is to address the root causes of maritime terrorism and mold political and socio-economic solutions to overcome them.

[14] This was the idea behind the SFI initiative led by the US.

Every player in the maritime supply chain must be made conscious of the importance of not only taking care of his own domain within the maritime supply chain but also to be on the look-out for anything out of place and suspicious and raise the red flag to others should they detect something amiss. They must realise that the strength of the chain is only as good as its weakest point. A strong sense of accountability and responsibility to maintain security in one's operational domain in the maritime chain is essential before players along the chain can develop awareness of the security situation in the entire chain. They should also be made aware that investing in improving security and being vigilant benefits them and can create value across the business functions throughout the entire maritime supply chain. The players along the chain should strive to invest in security by integrating security as a core business process rather than treating it as a peripheral issue. Investing in security often yields dividends to their business as smart security practices help protect their personnel, assets (fixed and in transit), brand and goodwill of their customers.

It would be counterproductive to live in fear and over exaggerate the threat of terror as it would just play into the hands of the terrorists and disrupt many aspects of our lives. While we could imagine all sorts of potential terrorist threats and worst-case scenarios, our resources and capabilities to counter them are finite and we need the maritime supply chain to operate with optimal efficiency to facilitate global trade and economic activities. But it has to be remembered that the price to pay for being tardy in securing the maritime supply chain could prove fatal to lives and damaging to assets and economic interests,[15] not to mention the potential of inflicting a political fall-out to governments. As such, there must be a nuanced approach to combating maritime terrorism; a risk-based security philosophy is more practical than a 'looking for a needle in a haystack' approach.

No one is immortal, but that does not mean we should leave things to chance. All the players along the maritime supply chain owe it to themselves to declare and treat maritime terrorism as, in the immortal words of Shakespeare, the 'chiefest enemy'.

[15] It was estimated that should shipping traffic along the Straits of Malacca, Sunda Strait, Lombok Strait and Makassar Strait were simultaneously blocked, the extra steaming costs to shipping companies could run up to US$8 bil. a year. See Ho, J. (2005), 'Maritime Security and International Cooperation', *Journal of the Australian Naval Institute*, 117, Winter 2005, 29–30. Meanwhile, the attack on Limburg was estimated to have inflicted a loss of US$3.8 mil. a month to Yemen's economy owing to the hike in insurance premiums for vessels visiting Yemeni ports and the loss of business due to the diversion of shipping traffic to other ports. See Burns, R. H. (2009).

References

Bateman, S. (2004), 'International Solutions to Problems of Maritime Security—Think Globally, Act Regionally!, *Maritime Studies*, November–December 2004.

Blanche, E. (2002). 'Terror attacks threaten oil routes', *Jane's Intelligence Review*, December 2002.

Borgu, A. (2004). 'Maritime Terrorism: An Australian Perspective', *Workshop on Maritime CounterTerrorism of the Observer Research Foundation*, 29–30 November 2004.

Bradford, J. (2004). 'Japanese Anti-Piracy Initiatives in Southeast Asia: Policy Formulation and the Coastal State Responses', *Contemporary Southeast Asia*, 26(3), December 2004.

Burns, R. H. (2004). 'Terrorism in the Early 21st Century: Maritime Domain', *IDSS Maritime Security Conference*, 20–21 May 2004.

Davis, A. (2008). Terrorism and the Maritime Transportation System : Are We on a Collision Course? Livermore, CA : WingSpan Press.

'Drawing the line between piracy and maritime terrorism', *Janes Intelligence Review*, September 2004.

Greenberg, M. et al (2006). Maritime terrorism : Risk and liability, Santa Monica, CA : Rand Corporation

Haberfeld, M. & Von Hassell, C. A. (2009). Modern Piracy and Maritime Terrorism: The Challenge of Piracy for the 21st Century. Dubuque, IA : Kendall Hunt Publishing.

Ho, J. (2005). Maritime Security and International Cooperation, *Journal of the Australian Naval Institute*, 117, Winter 2005.

Khalid, N. (2009). Raising of Security Alert in the Straits of Malacca : Lessons learned. Journal of Diplomacy and Foreign Relations. 11(1). 2010. 77-88.

Khalid, N. (2012). Sea Lines Under Strain : The Way Forward in Managing Sea Lines of Communication', *The IUP Journal of International Relations*, VI(2), April 2012. 57-66.

Mc Nicholas, M. (2007). Maritime Security : An Introduction. Burlington, MA : Butterworth-Heinemann.

Richardson, M (2004). 'The Threats of Piracy and Maritime Terrorism in Southeast Asia', Maritime Studies, November–December 2004.

Richardson, M. (2004). A Time Bomb for Global Trade : Maritime-related Terrorism in an Age of Weapons of Mass Destruction. Singapore : ISEAS.

Ritter, L. (2006). Securing Global Transport Networks, Burr Ridge, IL : McGraw-Hill.

Stephens, H. W. (1987), 'Not merely the *Achille Lauro* : The Threat of Maritime Terrorism and Piracy', *Terrorism: An International Journal*, 9(3).

Valencia, M. & Khalid, N. (2009). 'The Somalia Multilateral Anti-Piracy Approach : Caveats on Vigilantism', *The Asia-Pacific Journal : Japan Focus*, 8(4), 17 February 2009.

Young, A. &Valencia, M (2003), 'Conflation of Piracy and Terrorism in Southeast Asia: Rectitude and Utility', *Contemporary Southeast Asia*, August 2003, 25(2).

POST 2006 NEPAL: AN OBJECTIVE OVERVIEW

Nishchal N. Pandey[1]

No other country in South or Southeast Asia has so radically changed its political system in recent history as has Nepal. Nestled between the rising economies of India and China and endowed with Mt. Everest and Lumbini, the birthplace of the Buddha, it could easily have become one of the fastest growing economies of the sub-continent. Instead, it has suffered instability to such an extent that there have been 5 Prime Ministers in 6 years after the 'historic' change of April 2006, and still remains the poorest country in the SAARC region after, Afghanistan. After the loss of more than 13,000 innocent lives in the armed insurrection, there was much hope that with the Maoist decision to end the armed insurgency and participate in competitive multi-party elections in April 2008, stability would return, tourism would rebound and increased FDI would transform the rustic economy thereby injecting dynamism into the new republic. Unfortunately, the first-ever Constituent Assembly (C.A.) elected to draft a democratic, federal, and inclusive constitution did not complete its primary mandate when its term expired in May 2012. GDP growth remained as low as 4.5 percent in 2009, 4.8 percent in 2010 and further plummeted to 3.9 percent in 2011. Tragically, Nepal's main political parties entrusted to carry through the spirit of the people's movement have themselves fallen prey to an unceasing yearning for power in an eternal game of forming and dismantling governments, which has weakened the system and raised frustration among the common man. The terai,[2] that is the main granary and an industrial area, harbors more than 12 armed groups that compete with one another in abduction, looting, murder and explosions. And all major constitutional bodies currently lack leadership due to the absence of a legislature and a lack of consensus among the major parties.

[1] The Author is the Director of the Kathmandu -based Centre for South Asian Studies (CSAS) and a well- known academic and strategic analyst of Nepal.

[2] Note: Terai are the plains of southern Nepal bordering the Indian states of U.P. and Bihar.

There has been one major headway, however. Combatants of the People's Liberation Army (PLA) belonging to the Maoists who were stationed in UN monitored cantonments and later verified by a special committee have joined the army as envisaged by the Comprehensive Peace Agreement (CPA) signed between the state and the rebels in November 2006. The integration of 1,450 former Maoist fighters into the Nepal army marks a historic step. "With this, the system of 'one country, two armies', which had existed since the conclusion of the civil war in 2006, comes to an end. The fate of the former guerillas of the People's Liberation Army (PLA) had cast a shadow on Nepali politics over the last four years."[3]

This paper delves into the fault-lines of 'New Nepal' and analyses the roots of violence in Nepali society which have remained un-addressed despite of the radical transformation of the political system. While old wounds have yet to be healed, newer blemishes and scars have emerged. The breakaway Maoist party led by hard-liner Comrade Kiran has vowed that "it will launch a series of protests to oppose Indian investment in the hydro-power sector from next month (Nov. 2012) as these are more in favor of India than Nepal."[4] The same rhetoric was displayed by his mother party led by Prachanda and Dr. Baburam Bhattarai when the 'people's war' was initiated in February. 1996. In their 40-point demand list submitted to the then Sher Bahadur Deuba government, they raised almost the same issues of ultra-nationalism such as the "abrogation of the 1950 Treaty of Peace and Friendship and the Agreement of Tanakpur and the Mahakali water projects with India, the regulation of the open border between Nepal and India, the cancellation of Gorkha recruitment in the British and Indian armies, the initiation of the work permit system for Indians and a ban on Indian films."[5] It must be underscored however that the Maoist leadership kept on living in various hideouts in India through much of the insurgency period. If this trend of heaving anti-Indian sentiment continues, Nepali politics will not only go back to square one, but will also send ripple effects throughout the entire sub-continent. It will set-off high levels of uncertainty and unpredictability, and future developments will be

[3] Induction of Former Maoists into the Nepali Army should expedite much- needed economic development. (2012, Oct. 5). *Times of India*.

[4] CPN-Maoist against Indian Investment in Hydropower. (2012, Oct. 15). *The Kathmandu Post*.

[5] Shrestha, Chuda Bahadur (2004). *Nepal Coping with the Maoist Insurgency*, Kathmandu: Chetana Lok Shum Publisher. p. 106.

strongly influenced by the strategic maneuverings of India and China as they would not like to see a potential flashpoint emerging in an area that is so close to the Naxalite -affected states on the one hand, and the Tibet Autonomous Region on the other.

Background

Ten years of armed insurgency (1996-2006) have had a disastrous effect on Nepalese economy and society. Critical infrastructure such as schools, government offices, police posts, bridges, telecommunication towers and post offices were destroyed. Even hydroelectric plants were not spared. In a bid to tame the insurgents, the state doubled the strength of the army from around 45,000 to 90,000, increased defense expenditure from Rs. 2.58 billion in 1996 to Rs. 10.9 billion a decade later. The total budget for the Nepal Police also rose dramatically from a mere Rs. 2.36 billion in 1996 to Rs. 7.88 billion by 2006. However, by the end of the conflict, the police had abandoned 1035 police posts scattered all over Nepal.[6] As it was ineffective in countering the challenge posed by the insurgents, the government under G.P. Koirala decided to set-up a separate para-military force known as the Armed Police Force, in the year 2000. The budget allocated for development was diverted to implement emergency rule. Rising popular frustration in the hinterland, steadily narrowed Kathmandu's options. The economy suffered.

GDP growth during the conflict period, particularly after 2001 when emergency was declared, was sluggish. The average growth rate during the eleven year period from 1990 to 2000 was 4.8 percent, whereas it remained at 2.6 percent during the period between 2001 and 2005. Therefore, the economy kept losing an average of 2.2 percent GDP each year after 2001.[7] Altogether 20 district headquarters out of 75 were attacked by the Maoists. Together with the destruction of private property, a total of Rs 92.8 billion is estimated to have been lost during the period from 1996 to 2005. In fact, the economy lost an annual average of 6.3 percent of GDP over the

[6] *A Decade of Disaster: Human and Physical Cost of Nepal Conflict 1996-2005.* (May 2006). Kathmandu: Community Study and Welfare Centre. P. 126

[7] An Assessment of Economic Cost of the Ongoing Conflict in Nepal. (2009). Retrieved from http://www.fesnepal.org/reports/2005/seminar_reports/report_NEFAS_ConflictCost.htm.

preceding year as a result of the conflict.[8] During the decade of the conflict GDP fluctuated drastically. It was 4.8 percent in the financial year 1996/97, and reached a peak of 5.7 percent in the financial year 1999/00 before going down to its lowest level of – 0.3 percent in 2001/02.[9]

However, no marked improvement could be seen even after the Maoists joined mainstream politics, and much of this low level of confidence in the economy was due to the continuous political bedlam, power shortages, crises in the terai and strikes called by trade unions affiliated with one party or another. "Nepalese politics has long been about the acquisition of government resources for purposes of patronage as the people of various walks of life point at each level of government, a system that exists for seizing and diverting the country's resources to narrow rather than broader interests. Political parties have been part and parcel of this institutional syndrome."[10]

In fact, as soon as the people's movement of April 2006 was successful, the government began requesting funds for reconstruction and rehabilitation. However, this by itself was insufficient to rehabilitate and reintegrate those affected by the conflict and resurrect the ravaged economy. The bold decision by the Maoist leadership to shun armed insurrection and embrace competitive multi-party politics through the signing of the *Comprehensive Peace Agreement* was, surely, a welcome change that the people of Nepal and the international community both desperately wanted. Although it was achieved after much bloodshed and devastation, there was hope of lasting peace. The holding of elections for the country's first Constituent Assembly on April 10, 2008 was another landmark event in which the CPN (Maoist) emerged as the single largest party. The first elected Prime Minister under the republican order, Pushpa Kamal Dahal 'Prachanda', managed to collect record revenues during the tenure of the Maoist led government, exceeding its target by 31.7 per cent. The finance ministry collected 39.3 per cent more revenue at Rs 98.67 billion as per the year-on-year record.[11] However, his government was short-lived due to a miscalculated decision to sack the Army Chief-of-Staff which was not approved by the President. To save face, Prachanda resigned. Since then, other political parties have been constantly

[8] ibid

[9] Pyakuryal, B. (2007). *Nepal's Conflict: A Micro Impact Analysis on Economy*, Kathmandu: p. 24.

[10] Ghani, A., & Lockhart, Clare. (2008). *Fixing Failed States* London: Oxford University Press. p. 74.

[11] Record Revenue Collection. (2009, April 19). *The Himalayan Times.*

blaming the Maoists for espousing the dictatorial ambitions of 20th century communism. Relations between the private sector and the Maoist party, severely strained due to forced donations and labor problems during the course of the insurgency, did not improve even after the Maoists took charge of the government. "At a time when the government is seeking more investments from the private sector, entrepreneurs have expressed concern over increasing labor unrest, and political interferences which has weakened the capacity of the private sector."[12]

Therefore, despite high hopes, Nepal is still treading through a rough transition. The issues of federalism, the re-building of destroyed infrastructure, and the writing of an inclusive and democratic Constitution, within the now-lapsed, time-frame are critical issues that demand adept handling by all political forces. Unfortunately, the state has not been able to focus on these areas as a result of which popular frustrations are again rising. Highways are regularly closed by *bandhs* and strikes. Internal displacement is a huge issue as people move in their thousands from the villages to the district headquarters or to towns and cities considered 'safe' from the Maoists but the state is yet to create an enabling environment for them to return. Most of the forcibly confiscated property still remains to be returned by the Maoists.

There is, moreover, an acute shortage of electricity all over the country which has resulted in the closure of several important industries. In addition even Kathmandu has been grappling with erratic supplies of essential commodities – like petroleum, cooking gas and vegetables. The capital, Kathmandu, experiences 18 hours of daily load shedding during winter, which is ironical in a nation that has 83,000 megawatts of unharnessed energy potential. While impinging on the overall economic activity of the country, these issues are negatively influencing macroeconomic stability and the regular budget outlays of the government, which has been criticised for huge expenditures on unproductive programs. With the dissolution of the legislative parliament in May 2012, the government has only a six-month budget at hand and is unable to pass a full-fledged budget for the whole year.

[12] Political Interference, labor unrest behind slowing economy. (2012, Oct. 12). *Republica National Daily.*

Rough Road to Federalism

One of the foremost challenges that the country faces is that the Interim Constitution has already stipulated that Nepal will henceforth be a 'federal republic' but the modalities of federalism, the basis of such federal units and their financial sustainability have yet to be examined. "The process of people's political mobilisation during the last ten years of insurgency had sharpened the sense of identity among disparate ethnic groups and shaped their political views."[13] A centralised state for over 200 years was badly in need of restructuring but instead of looking at various viable models of federalism, some political outfits want federal states carved out on the basis of ethnicity. This is a highly explosive design that is certain to backfire as Nepal has more than 102 recognised ethnic groups but none of those group(s) in whose name the states are to be formed constitutes a majority. The Brahmins and Chhetris that comprise more than 32 percent of the total population of the country are to be deprived of any state of their own if some of the proposals submitted to the erstwhile C.A. were to be implemented. Minority appeasement tactics to win over vote banks is a disease that has already sneaked into Nepal from neighboring Uttar Pradesh but what the country's political leaders need to draw lessons from is the recent success story of Bihar which has curbed crime, cleaned up bureaucratic red-tape and is now recording a 13.1 percent GDP growth rate.

It is true that the federal debate was orchestrated in light of the enormous pressure from Madhesis and groups from the indigenous nationalities who rightly impugn the state as having marginalised them in all spheres of activity including employment in government jobs. This led to the Madhesh upheaval in 2007 where there were demands for better representation of Madhesi people in the security services, government, politics and the economy. In the elections held the following year, the Madhesi parties secured less than the 3 major parties - the UCPN (Maoists), CPN (UML) and the Nepali Congress but emerged as power brokers. Taking the cue from their sudden success, other fringe parties and criminal elements operating in the Indo-Nepal border also began promoting the

[13] Pattanaik. S & Nayak, N. (2008). Post-Election Nepal: Maoist Success and Challenges Ahead. In Ashok K. Behuria (Ed.), *India and Its Neighbours: Towards a New Partnership*. (p. 45). New Delhi: Institute of Defense Studies and Analyses.

Madhesi cause purely for personal, petty gains resulting in law and order of the terai districts being the direct casualty. "The security vacuum in the terai districts marked by a feeble presence of police and other border regulating agencies known for their corruption has made this uniquely open border as one of the most illegally trafficked border in the world. The poorly guarded open borders are increasingly tempting unscrupulous parties to engage in a range of criminal activities. The post conflict uncertainties and the erosion of law and governance have indeed raised the specter of criminal activities engendering the security of both India and Nepal."[14]

Therefore, the assertion of the ethno-linguistic chauvinism of the Madhesis is a critical element to factor in the future stability of Nepal. There is a real danger that if this ardor of ethnicity-based federalism and the obscure demand of 'self-determination' is not properly handled, the slow balkanisation of Nepal will become an eventuality. Some academics however feel that "societies where federalism was introduced in an open environment, based on mutual negotiations and compromises between conflicting parties have unified countries and led to the consolidation of democracies. The open environment in those societies not only led to negotiated settlements between various groups and regions but also allowed for progressive demands to be aired and met in successive years."[15] How and by whom these conflicting issues will be dealt with have a bearing also on the security of Tibet and North India essentially because ethnic groups are linked across the border(s) by matrimony, religion and language. For instance, there are more Maithili speaking people in India than in Nepal and an autonomous region of the Sherpa community in Nepal could also bandwagon with their kith and kin across the border in Tibet. Each state could also erect its own security force which may compartmentalise the professional units of the Nepal Police and other vital organs of the state. "There is a huge demand and political pressure to disintegrate the Nepal Police on ethnic and regional basis so that it may save political parties locally and regionally."[16] If this happens, the law and

[14] Upadhaya, A., (2011). Conflict in Nepal and its Transnational Ramifications. In Raghavan, V.R. (Ed.), *Internal Conflict in Nepal* (p. 133). New Delhi: Vij Books India Pvt. Ltd.

[15] Lawoti, M. (2010). Federalism, the Right to Self-Determination and National Security. In Bhattarai, R. & Wagle, G. (Eds.), *Emerging Security Challenges of Nepal*. Kathmandu: NIPS. p. 184.

[16] Thapa, R.R., (2011). Law Enforcement in Post-Federal Nepal. In Pandey, N.N. & Delinic, T. (Eds.) *Nepal's National Interests*, Kathmandu: CSAS & KAS. p. 250.

order situation which is already in disarray could further plummet leading to its total politicisation.

Nepal, which is a multi-lingual, multi-ethnic and multi-caste country with an 80 percent Hindu populace, has historically been a tolerant society. Since 2006, it has been officially declared 'secular'. In 2008, a Hindu fanatic planted a bomb in the Church of Assumption near Kathmandu killing several people while other grave attacks against Muslim religious leaders have also been reported. A combination of intellect, sagacity and a finely balanced policy of ensuring freedom to all religious groups without creating a sense of estrangement to among the majority is the need of the hour which again warrants wisdom from all political forces.

Macroeconomic Performance

The foremost cause for a very low industrial output has been the political bedlam in the terai, which is the main granary and also the industrial belt of Nepal bordering U.P., Bihar and Uttarakhand. The turmoil began in early 2007 as the terai parties began demanding better representation, more rights and a budget for the Madhesis.[17] Terai occupies 23 percent of Nepal's total area, comprises 24 out of 75 districts in the country, and holds 48.5 percent of the total population. 74 percent of paddy cultivation is in the terai. It is famous for cash crops such as sugarcane, jute, tobacco, tea and pulses. Staples such as paddy, wheat and maize are its main agricultural produce.[18] Its forests provide *sal* wood and commercially valuable bamboo and rattan. It also controls the chief supply route to India. All daily essentials from India to cities such as Kathmandu and Pokhara have to transit through the terai districts. Continuous disruption in vehicular movement, especially at the transit points has affected the Nepali industrial sector. For instance, during the agitation launched by the Madhesi Janadhikar Forum (MJF) and Jantantrik Terai Mukti Morcha (JTMM) in Feb. 2007, thirty-six out of 40 industrial units were closed due to a scarcity of raw materials in the

[17] Note: Madhesis are people of Indian origin who live in Nepal's southern area bordering India. The word "terai" and "Madhesh" have been used interchangeably. There are a substantial number of people from the hills too who have settled in the terai.

[18] Rakesh, R.D., (2007). *Murder of Madhesh*. Kathmandu: Safari Nepal Publishers, P. 9.

Hetauda industrial zone of Makawanpur district. Among them, five were multinational companies including Colgate Palmolive, Unilever Limited and Alcoa CSI Pvt. Ltd. The import of raw materials from India and third countries was obstructed. Colgate Palmolive shut all activities after it failed to receive raw materials for two weeks. An official stated that imported goods were held up at the Birgunj customs post for a week. Another multinational, Unilever Limited also halted manufacturing as goods produced at the plant could not get to the market as they were held up at the Birgunj Customs office for more than a week.[19]

Although these industries have since resumed production, the Jyoti Spinning Mill closed down completely, citing unsafe operating conditions and daily power cuts. It was the first modern spinning mill in the country established in 1989 in Parwanipur with 1200 workers. Surya Nepal Garments, an Indian multinational company in Biratnagar also closed down on May 28, 2009 due to a dispute with the labor union. The increasing trend of demanding unwarranted wage increases, calling strikes on the flimsiest of grounds and then blocking vehicular traffic along the highway just to coerce the government into making a deal has increased the cost of goods, reduced competitiveness and impeded economic growth. Insecurity in the terai, unpredictability of power supplies and raw materials together with waning harmony between labor and industry have adversely affected the industrial sector.[20] This is one of the most important issues confronting contemporary Nepal and unless we are able to create an investment friendly climate, ensure the safety of enterprises, employ qualified CEOs in relevant businesses, and provide basic minimum requirements such as power, road accessibility and other infrastructure, very little can be expected by way of foreign investment. Nepal must draw lessons from the sorry predicament of the state of West Bengal where similar issues hampered foreign investment for over 3 decades of communist rule.

[19] Thirty Six industries including multinational companies closed down in Hetauda. (March 15, 2007). Retrieved from http://www.nepalbiznews.com/newsdata/Biz-News/hetaudaindustrialareanews.html.
[20] See Three Year Plan Document, National Planning Commission, >www.npc.gov.np< 2008.

Tourism & Remittance

During the decade of conflict no other sector of the economy was hit as severely as tourism. Arrivals began to slide not only due to fighting along famous trekking routes and tourist sites, but also because of a series of mishaps that Nepal witnessed in the last decade. The hijacking of IC 814, the Royal massacre of 2001, the endless strikes and negative publicity in the international media coupled with travel advisories that 'Nepal is not a safe destination' forced tourists to steer clear of Nepal. This, in turn, led to the closure of several hotels in Kathmandu and Pokhara. A nation famous for some of the world's highest peaks and a haven of peace, where the Buddha was born, had turned into a deadly war zone and it was only natural for tour operators to look for alternative destinations. Even after the political change of 2006, the country experienced one political crisis after another. In May 2010, the seven day closure called by the UCPN (Maoist) occurred during the summer vacations for schools in India, thus directly affecting tourism. Gross foreign exchange earnings in convertible currency from tourism stood at US$ 230.6 million in 2007. It represented an increase of 41.7 percent from 2006. The year 2011 witnessed a slight increase in tourist inflow but this trend needs to be sustained.

Nepal relies heavily on the remittances sent by its manpower that works in the Gulf, South Korea, and Malaysia. The youth who escaped the ravages of the insurgency, worked hard as laborers in these distant places but have been earnest in regularly sending their earnings back to their families in Nepali villages thus sustaining the economy even during pressing times. An estimated 2.2 million Nepalese live and work in these countries at present. On average the Nepali migrant workers earn around Rs 438.38 billion annually. Nepalese working in the Gulf countries – Qatar, Saudi Arabia and the United Arab Emirates – earn around Rs 319.5 billion followed by Malaysia (Rs 76.20 billion), South Korea (Rs 7.24 billion) and Kuwait (Rs 6.27 billion). About 1.5 million Nepalese work in Qatar, Saudi Arabia and the United Arab Emirates while 500,000 are in Malaysia, followed by 8,500 in South Korea and 40,000 in Kuwait. Maintaining the national economy through remittances as a source of income is not a dependable option, as there are other social ramifications to consider, like the health of the workers, the increasing number of broken families, etc. However, for now, this seems to be the only sector that is faring well.

Conclusion

Nepal is yet to settle down despite the abrogation of the 1990 Constitution, the holding of the Constituent Assembly elections, the declaration of a republican order and the formation of five different governments since 2006. Minimising the challenges of a transition that is prolonging and boosting a sense of security among the populace can be done only if the political parties exhibit maturity and evolve a healthy political culture. Since a constitution could not be drafted by the C.A. and the country is now devoid of a parliament, it is highly probable that Nepal will slide further into instability and unpredictability. At least, if a broad national consensus can be reached on basic issues such as foreign and economic policies, vital institutions can still function until the political situation is resolved.

VERNACULAR PRESS AND REPORTING CONFLICTS

Ranga Kalansooriya

ABSTRACT

Media always plays a key role in democracies, but once democracy is challenged media, too, face multi-layer dilemmas. Reporting conflicts becomes a conflict itself to media practitioners. In a conflict theatre, democratic norms and values are challenged and the media's attempts to protect vulnerable democracy results in heavy costs – even to the life of journalists and media practitioners. The vernacular press is the most volatile but also the most important segment of such a conflict theatre due to its outreach, accessibility and ability to influence society at large.

Keywords: *Global trends in news journalism, influencing factors, ethics, standards of vernacular press, news in conflicts, enemy image*

Introduction

Democracy is impossible without a free press (Baker, 1998) yet the media is always accused of being politically allied, ethnically biased and agenda driven, mainly when reporting conflicts. These accusations get more advanced when it comes to reporting terrorism, both at local and international contexts.

It is an undeniable fact that the media plays an extremely vital role in defusing tensions, managing conflicts and establishing democracy. As Kurspahic (2003) argues, making the independence of the media is an important part of future peace agreements and one of the must-do requirements for international acceptance of states in transition. But the real challenge is convincing the media to adopt this independence whose commercial side is necessarily a blending of two separate disciplines: business and journalism (Herrick; 2003). Apart from the commercial side, the media has a strong political agenda as well.

Media in conflict theatres is often accused of being ethnically, politically or religiously biased or polarised. However, it is biased on commercial terms to a greater extent. Many aspects such as market forces, the political alignment of ownership, readership influence and the lack of professional standards among journalists and editors are perceived to be the root causes for this phenomenon.

This paper is aimed at shedding a critical light on the role of the vernacular media in exploring whether it has a role in preserving a country's democracy by defusing the prevailing ethnic, political or religious tensions and establishing harmony between the conflicting parties. The main focus of the paper is news journalism, rather than features or any other form of journalism.

News and News Reporting

Information, education and entertainment are the cardinal components of the media of which information, as in the formation of 'news', reaches the public. Some would argue that news and information are two different components of media – based on public response, but there exists a fine line demarcating the two.[1]

An independent media is the pillar of true democracy and no other institution does what journalism does, namely to "inform, monitor, and critique" public affairs (Stepp; 1996). To the extent that papers and stations try to "fix government through journalism" or "substitute journalism for government" they depart from their unique duties to provide checks on government that are critically important to democracy, argues Stepp.[2] Though he, in his academic commentary, does not deeply engage with the concept of news in the field of media, many scholars have argued that the impact of news is the cardinal element in shaping public opinion at large.

News, one of the most important forms of information imparted by the mass media (Roy; 2005), is considered one of the most important components that shapes public opinion (Shrivastava; 2003). It also makes people feel they are part of a bigger network of people, or a larger community which could be derived through a formula where people and their actions

[1] Information is something that would generate an immediate response from an individual. One can receive information through news which is more colourful, creative and attractive, according to Prof. Shrivastava of the Indian Institute of Mass Communication (personal interview).

[2] Carl Stepp,"Public Journalism: Balancing the Scales," American Journalism Review 18 (1996): p40.

are conjoined with the readers' interest for which the news is generated (Roy; 2005).[3] But according to Dzur (2002), news is more than the information that the public wants. According to him, the mandate of news goes beyond just reporting but generating public discourse. More controversial than the re-conceptualisation of what is newsworthy, so that it includes non-elite stories and purposeful news, is the belief that to promote public deliberation journalists must do more than report the news, and should broaden their role to include helping the public convene and deliberate about public affairs, Dzur says, adding that news journalists should play the role of the neutral referee in such public deliberations which were derived from the news he relayed to the public. Of course, the metaphor is not entirely apt, since referees do not influence the rules of the game and seldom urge the players onto the field. Like referees, though, journalists would immediately lose their particular role-based authority if they were to actively root for one side, Dzur argues.

But it is seldom that the journalist himself/herself takes the decision to be one-sided. In the corporate business of news media, and also in the Asian context where media is a value- added commodity in gaining political power, the concept of objective news reporting has different variations and interpretations. Several writers argue on different agendas in news reporting in this context, especially on market interest, business models, corporate influence and political agendas.

Kressel (1987) argues that the judgments of media bias rest upon three socio-psychological processes: a general, cognitive confirmatory bias in judging evidence, a tendency for deeply involved partisans to have a wide latitude of rejection, and a tendency for partisans to perceive (and misperceive) media in accordance with their overall views. At the same time he feels that the media criticism may also be understood as a partisan, political tool. While the media do have an obligation to adhere to certain journalistic norms and standards, it is difficult -if not impossible- to invoke these norms without making normative and conceptual judgments, Kressel says. In fact, something similar to Herrick's concept of media business was

[3] Roy Barun in his formula [People + action + reader's interest = News] argues that all these three adding components are equally important in creating news.

tried, unsuccessfully, by several major media moguls in India several years ago, after which they returned to the basics of news media management.[4]

Media owners are not the only stake holding factions that attempts to influence media, news journalism in particular. Herbert (2001) argues that politicians, statesmen, businessmen (advertisers), and the rich and influential throughout the world have tried to change the face of journalism and what it publishes. However, with the advancement of the New Media in this digital age, he says, their influence has becomes redundant. "Authoritarian control over media still exists in many countries. But because of the way new technology allows information to be transmitted and shared by journalists and others worldwide, governments are finding censorship increasingly difficult to maintain,"[5] he says.

Vernacular press and conflicts

The Oxford Dictionary explains the term 'vernacular' as the 'ordinary language of a country or district.'[6] Though, in contemporary media studies the term 'press' is used often to refer to all forms of mass communication of information and opinion on affairs of current interest (Peiris, 1997: 01), press – by and large in general usage – is described as the print media. Thus, the vernacular press is considered the local language print media in a country. In fact, it is the most read and accessed print media compared to English publications in any country. Thus, its impact is immense on its readership, which is the majority of country's population, no matter what native language they use.

There is a general consensus that all conflicts must be seen in a regional context (Loewenberg; 2007). Even in internal conflicts, neighboring states are almost always involved directly or indirectly whether because of minority/majority populations across national borders, the harboring of rebel

[4] Some major Indian newspaper companies like the Indian Express made several attempts to reshape news in-line with advertising interests and also through new marketing strategies where editors were advised to emphasise marketing concepts when presenting news of the day. However, this attempt did not bring in the expected commercial results to the corporate ownership prompting them to return to the basic concepts of news presenting.

[5] John Herbert, *Practicing Global Journalism*, (Oxford, 2001), p 8

[6] The Oxford Mini-reference Dictionary and Thesaurus; Oxford University Press; p 707

groups, fleeing refugees, state security concerns, political interests etc, says Loewenberg. Against this backdrop, the importance of the local language media is critical in disseminating information to the local population in their own language.

The mass media has played an increasing role in mobilising population groups behind their leadership in violent conflicts. In the former Yugoslavia, Rwanda and many other countries, the local media have turned a blind eye to societal inadequacies and the political or economic root causes of conflicts. During the escalation of conflicts, the media have contributed to it by perpetuating prejudices, stereotypes and the hate speeches against other parts of the population using ethnic, religious or cultural identities as rallying cries. (Bonde; 2007).

In pre-conflict, during -conflict and post -conflict environments, Bonde identifies several areas of media for intervention; content, media structure, media legislations, ethics and capacity building – a process that would include all key stakeholders and institutions in a democracy, Parliament, Government, regulatory bodies, broadcasters and print media (ownership), media (at large), minority and human rights NGOs.

The key feature in media biasedness is the portrayal of the enemy image – mainly in the guise of 'us vs. them' concept. This phenomenon is widely seen in the vernacular press when compared to the English press for multiple reasons.

Patriotism plays a pivotal role in portraying the enemy image – mainly in demonising the enemy. Some social scientists explains this as a socio-psychological issue while another school of thought believes this to be a propaganda methodology employed by the state or other influencing sector. Kelly & Michela (1980) and Ross (1977) both argue that the creation of a borderline between 'us' and the 'other' is a socio-psychological mechanism that occurs in all human relations; in the neighbourhood, community and society, people will include some but exclude others on the basis of different criteria. Eventually nations start to define other nations as the 'other', according to Ottosen (1995). Philip Knightley (1975) describes how an important element in war-reporting is to 'demonise' the enemy and to portray him as 'an animal in human disguise'.[7]

[7] Ottosen Rune, *Enemy images and Journalistic Process*, Journal of Peace Research, Prio – Oslo, 1995 p 98

Thus, the journalistic practice get twisted and distorted with a hidden agenda where the readership is heavily affected. This portrayal of the enemy image by the agenda-guided media against the other was clearly visible in the Balkans conflict as explained in above paragraphs. Also it was obvious – mainly in the vernacular press – during many conflicts around the world, including the Gulf War, global way against terror and also that of Sri Lanka.

In these conflict environments, the stereotypes in the media can legitimise violent actions even in news reporting, with the 'news slant' and rhetoric applied to the stories to enhance the prevailing enemy image and systematically change the mindset of the public (their own clientele) against 'the other.'

To gain a deeper understanding of enemy images in everyday journalism, one has to analyse a sample of newspapers over a longer time-span, including periods when the situation is more 'normal' than during overt conflicts. The extent to which linkages can be found during commercial pressure and political frames of reference should also be examined. (Ottosen; 1995)

Being patriotic or loyal to your own 'side' makes it easy for the journalist to portray the enemy image against the 'other' – but putting his own practice of the profession in question says Herbert (2001). He argues that the dilemma faced by journalists by being loyal to 'their own side' without allowing themselves to get caught up in the propaganda has been in existence for a long period, until Vietnam provided a better lesson. Herbert says:

> "In Vietnam, the military, as they had done before, expected journalists to be loyal to their own side. For a while this probably was the case. The Western allies were the good guys; the Vietnamese weren't. But then came the 1968 Tet offensive when the journalists reported what they saw, not what the military wanted them to see,"[8]

Another classic case in studying the concept of portraying the enemy image in the media is the Israel – Palestine conflict. According to (Kressel 1987) the critiques of media coverage offered by pro-Arab writers and pro- Israel writers contain some structural similarities. Both groups cite: (1) unbalanced and disproportionately unfavorable coverage, (2) distorted

[8] John Herbert, *Practicing Global Journalism*, (Oxford, 2001), p 36

and untrue media portrayals of the conflict, (3) prejudice and stereotyping, (4) employment of double standards, and (5) various unfair political and organisational barriers to an objective coverage. In addition, pro-Arab commentators have highlighted quantitative under-representation in media coverage. Pro-Israel writers have discussed limitations inherent in the media themselves-such as the broadcast media's weakness at handling the contextual background, Kressel argues.

Conclusion

The media is a powerful tool in shaping the public mindset, and the vernacular media has the highest impact among others. Though the broadcast media – especially the radio - plays a major role in its outreach, the print media (press), too, is significant in providing more analytical and thought provoking content.

The vernacular press is extensively challenged in conflict theatres, as its content has comparatively long shelf value and tangible accessibility. It is directly targeted by various interest groups and parties to the conflict in shaping public opinion as well as disseminating information, mostly on propaganda basis.

In contrast, the media has its own challenges. Poor professional standards and ethics, the influence of the ownership, the lack of understanding of the conflict, politically driven agendas and also the ethnically or religiously biased vernacular press that could be more powerful than a lethal weapon.

The most dangerous phenomenon is when the media becomes a party to the conflict, abandoning its due watchdog role. Then it becomes an "us against them battle" not only on the conflict ground but even in the news pages themselves. This was the case in many conflicts in places such as the Balkans, Sri Lanka, the Middle East and elsewhere. The portrayal of the enemy image by demonising the other party becomes the core business of its content in what is termed 'Patriotic Journalism' which totally contradicts the basic norms of journalism. Enhancing professional standards, minimising ownership influence, sensitising the journalist and media gate-keepers to conflict through capacity building are among the recommended remedies in addressing this issue.

Bibliography

Alam Imitiaz et al, Media and Peace in South Asia (2006), SAPNA, Lahore – Pakistan

Anastasijevic and Borden et al, Out of Time (2000), IWPR, Belgrade

Bose Sumantra; States, Nations, Sovereignty – Sri Lanka, India and the Tamil Eelam Movement (1994), Sage Publication, New Delhi

Carl S. Stepp," Public Journalism: Balancing the Scales,"American Journalism Review 18 (1996):4

Crighton Alistair, Macedonia; : The Conflict and the Media (2003), Macedonian Institute for Media

Dennis, Herrick, *Business Dynamics of Journalism*, Blackwell Publishing Company, USA, 2003

Dyal and Sahai et al (edited), Media and Public Interest in South Asia (2005), FES-UNESCO-AMIC India, New Delhi

Feintuck, Varney Mike et al, *Media Regulation, Public Interest and the Law*, Edinburgh University Press, Edinburgh, 2006

Fleming, Carole et al, *An Introduction to Journalism*, Vistar Publication, New Delhi 2006

Frost, Chirs, *Reporting for Journalists*, Routledge, London & New York, 2002

Galtung Johan; An Introduction to Conflict Work (2007), Ravaya Publication (Sinhala Edition)

Ghai Yash; Autonomy and Ethnicity – Negotiating Competing Claims in Multi-Ethnic States (2000) Cambridge University Press

Glover, Stephen, *Journalism Secrets of the Press*, Penguin Group, London, 1999.

Gunasekara H M, Media as Bridge Maker (1997), FES Colombo

Herbert, John, *Practising Global Journalism*, Focal Press, Oxford, 2001

Kazimir Velimir Curgus et al, Hate Speech in Yugoslav Media (1997), Belgrade Media Center

Kurspahic Kemal, Prime Time Crime – Balkan Media in War and Peace (2003), USIPP, Washington DC

Lewis, Jon, *The Mammoth Book of Journalism*, Robinson, London, 2003

Loewenberg and Bonde et al, Media in Conflict Prevention and Peacebuilding strategies (2007), Deutsche Welle

Peiris G H, Studies on the Press in Sri Lanka and South Asia, (1997), ICES, Kandy

Phadnis Urmila and Ganguly Rajat; Ethnicity and Nation-building in South Asia (2001), Sage Publication New Delhi

Raine Mary; Informed Democracies (2003), UNESCO and CPA Publication

Rotar Nada Zgrabljic et al, Media Literacy and Civil Society (2006), Media Center – Sarajevo

Roy, Barun, *Beginners' Guide to Journalism*, Pustak Maha, New Delhi, 2005

Samaranayake Gamini; Political Violence in Sri Lanka (2008), Gyan Publishing House New Delhi

Sen Amartya; Identity and Violence – The Illusion of Destiny (2006), Penguin Publication

Shrivastawa K M, News Reporting and Editing (1991), Sterling Publishers, New Delhi

Siroka Jugoslava, Ethics and Journalism (2005), Media Center Belgrade

Sivathamby Karthigesu; Being a Tamil and Sri Lankan (2005), Aivakam Publishers Colombo

Smiljanic and Dikic et al, Best of Sarajevo Notebooks (2008), Slovenian Ministry of Foreign Affairs

W L Bennett; News: The Politics of Illusion, New York: Longman (1988)

‘THE EVOLVING ROLE OF THINK TANKS IN COUNTERING EXTREMISM AND TERRORISM’

Rohan Gunaratna

Introduction

To counter violent extremism, over 100 think tanks are currently engaged in teaching, research, networking and outreach activities.[1] The ability of think tanks to develop excellence and also influence both government and community responses to security threats vary.

While some specialist think tanks work exclusively on violent extremism, others work on security in general, including terrorism and counter terrorism. In addition, one can also argue that if countering violent extremism is a discipline, it should be based at an academic institution else it may lack the necessary theoretical and methodological rigor and an interdisciplinary approach.[2]

The focus of most security think tanks is to work with governments where they mostly conduct contract research and engage in policy advocacy on behalf of governments. But, in addition to working with governments, it is also paramount for think tanks to work with community partners to engage susceptible communities vulnerable to extremist ideologies. By helping community organisations to counter extremist ideology and promote moderation among their communities, think tanks help communities to build social resilience. Future think tanks can play an appreciable role in creating an environment hostile to threat groups and unfriendly to supporters and sympathisers.

[1] Benjamin Freedman, “Terrorism Research Centres: 100 Institutes, Programs and Organisations in the Field of Terrorism, Counter-Terrorism, Radicalisation and Asymmetric Warfare Studies,” Perspectives on Terrorism, Vol. 4, No 5 (2010) <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/123/html> <Accessed August 27, 2012>

[2] Interview, Bruce Hoffman, Director, Center for Security Studies, Georgetown University’s Walsh School of Foreign Service, August 15, 2012

The First Generation Think Tanks

Spurred by the beginning of the contemporary wave of terrorism in 1968, the first generation of counter terrorism think tanks originated in the West and in Israel. RAND staff Brian Michael Jenkins, since 1972, and Bruce Hoffman, since 1981, have systematically studied terrorism. While Jenkins previously served in the US Special Forces in Vietnam, Hoffman was an academic specialist with field experience. They built and maintained the first international terrorism database. Since then, over forty years, RAND's reputation as a world leader in research on terrorism, counterterrorism, counterinsurgency and homeland security has grown.

In the UK, the discipline of terrorism studies was founded by Paul Wilkinson. Wilkinson was previously associated with and directed the Research Institute for the Study of Conflict and Terrorism (RISCT) in London that functioned from 1989-1999. Together with Hoffman, Wilkinson established the Centre for the Study of Terrorism and Political Violence (CSTPV) at the University of St Andrews in 1994. In addition to hosting the RAND Terrorism Chronology and advising governments, CSTPV offered counter terrorism courses at the undergraduate and postgraduate levels.

As much as the developments in Northern Ireland created the impetus for the creation of a counter terrorism capability in the U.K, the developments in the Middle East prompted the Israelis to create a similar capability. In 1996, the Institute for Counter-Terrorism (ICT) was founded at the Interdisciplinary Center (IDC), Israel's first private university. ICT offered counter terrorism courses at undergraduate and postgraduate levels.

The National Memorial Institute for the Prevention of Terrorism (MIPT) was created in response to the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995. Until 9/11, it was the worst terrorist attack on US homeland and MIPT dedicated itself to the training and professional development of nearly a million American law enforcement officers, both in crime and terrorism prevention. With the exception of the US Library of Congress, the MIPT's Lawson's Library hosts the largest online repository of homeland security and terrorism data for use by US law enforcement.

The first counter-terrorism research think tank outside the West and Israel was established in China. The China Institutes of Contemporary International Relations (CICIR) launched the Center for Counter-Terrorism Studies in 2000. Considered the first academic research institution specialising in counter-terrorist studies in China, the CICIR also focused on transnational organised crimes, proliferation of weapons of mass destruction, etc.[3] The Center established databases, published research papers and held domestic and international seminars.

Second Generation of Think Tanks

Spurred by 9/11, the second generation of think tanks emerged both in the global north and south. In the wake of Al Qaeda's 9/11 attacks and the disruption of the Al Jemaah Al Islamiyah plot to attack Singapore in December 2001, the Government of Singapore reassessed the threat of terrorism. In July 2002, a terrorism research programme was established within the Institute for Defence and Security Studies, now the S. Rajaratnam School of International Studies (RSIS), at Nanyang Technological University. The programme was subsequently upgraded into the International Centre for Political Violence and Terrorism Research (ICPVTR) on February 20, 2004. A critical node in global threat research, ICPVTR's functional and regional analysts cover Asia, Africa, Europe, North America and the Middle East. Analysts are drawn from a range of academic backgrounds and government agencies and also include Muslim religious scholars. While ICPVTR seeks to maintain its unique cultural and linguistic diversity, it has a strong Muslim representation - of more than fifty percent among its staff - that enables it to put into context Islamic concepts which have been misrepresented in radical propaganda espoused by terrorist ideologues. Since 2003 the ideological response unit of ICPVTR, spearheaded and staffed by clerics, built government capacities to rehabilitate terrorists and counter extremism in communities.[4]

[3] China Institutes of Contemporary Relations, <http://www.cicir.ac.cn/english/organView.aspx?cid=382>, <Accessed August 27, 2012>

[4] Muhammad Haniff Hassan and Mohamed Redzuan Salleh, Jihadism studies in counter ideology: Time for initiation in universities, RSIS Commentaries ; 085/10; S. Rajaratnam School of International Studies, July 28, 2010 < http://www.rsis.edu.sg/publications/Perspective/RSIS0852010.pdf> ,<Accessed August 27, 2012>

The United States Military Academy (USMA) at West Point established a Combating Terrorism Center (CTC) on February 20, 2003. Russ Howard, a former Special Forces Officer, who was the Head of the Department of Social Science, was its founding Director.

The Fletcher School for Law and Diplomacy created the Jebsen Center for Counter Terrorism in 2005. The first graduate-only school of international affairs in the United States established in 1933,[5] the Fletcher School is at the Tufts University in Boston. Due to a lack of continuity in funding, the Center was closed down in 2006 but Richard Shultz, a professor of international politics, and other academics at Fletcher retain significant expertise on counter terrorism and counter insurgency.

The Australian government supported the development of university and non-university think tanks to counter violent extremism in Australia. The impetus for this support was the terrorist attack in Bali in October 2002 that killed 202 persons including 88 Australians and the continuing threat on its own soil. The Centre for Policing, Intelligence and Counter Terrorism (PICT) at Macquarie University, Australia was established in 2005.[6]

The Global Terrorism Research Center at University of Monash was established in 2006. Adam Dolnik, an ICPVTR alumnus and a Ph.D. from RSIS, served as the Director of Terrorism Studies at Wollongong University's Centre for Transnational Crime Prevention training a new generation of Australian and international scholars and practitioners.

To guide counter terrorism research to secure the US homeland, several government institutions have provided grants to US and foreign think tanks. They range from the United States Institute of Peace, Office of Naval Research and the Department of Defence. A U.S. Department of Homeland Security (DHS) Center of Excellence - The National Consortium for the Study of Terrorism and Responses to Terrorism (START) - was established at the University of Maryland at College Park by Gary LaFree in 2005.[7]

[5] The Fletcher School, Tufts University, <http://fletcher.tufts.edu/About/Fletcher-History>, <Accessed August 27, 2012>

[6] Centre for Policing, Intelligence and Counter Terrorism, Macquarie University; <http://mq.edu.au/about_us/faculties_and_departments/faculty_of_arts/centre_for_policing_intelligence_and_counter_terrorism/about_pict/>, <Accessed August 27, 2012>

[7] The National Consortium for the Study of Terrorism and Responses to Terrorism, University of Maryland, <http://www.start.umd.edu/start/about/overview/mission/>, <Accessed August 27, 2012>

The International Centre for the Study of Terrorism (ICST) at the Pennsylvania State University was launched in London on May 20, 2006. Strong in social and behavioural science study, ICST's multidisciplinary and cross-national teams conduct contract research both for government and the private sector.[8]

The International Centre for the Study of Radicalisation (ICSR) was launched in London in January 2008 with Peter Neumann as its Director who also co-directs the MA program in Terrorism, Security and Society at the Department of War Studies.

The International Centre for Counter-Terrorism at The Hague was launched on May 31, 2010. ICCT was founded and is supported by a unique partnership comprising three renowned institutions based in The Hague - the T.M.C. Asser Instituut, the Netherlands Institute of International Relations 'Clingendael' and the Centre for Terrorism & Counterterrorism of Campus, The Hague/Leiden University. Supported by the Dutch Ministry of Foreign Affairs and other donors, Peter Knoope has been the director since ICCT's inception.

Non-University Think Tanks

Several hundred non-university affiliated think tanks also study and research methods to counter violent extremism. While some are government or government- supported, others are corporate or privately- funded think tanks registered as NGOs. The NGO think tanks are the ones close to the ground working in conflict zones and with access to serving and former violent extremists. With funding from western governments including Australia, Japan and other donors, they conduct field research, publish research papers, train and engage in outreach activity.

Established in 1997, the Institute for Conflict Management (ICM), New Delhi, is South Asia's leading counter terrorism and counter insurgency think tank. The Pak Institute for Peace Studies (PIPS), an independent, not-for-profit, non-governmental research and advocacy think tank was established on January 10, 2006.[9] Located in Kabul, Afghanistan, the

[8] International Center for the Study of Terrorism, The Pennsylvania State University, <http://www.icst.psu.edu/About.shtml>, <Accessed August 27, 2012>

[9] Pak Institute for Peace Studies, <http://san-pips.com/>, <Accessed August 27, 2012>

Centre for Conflict and Peace Studies (CAPS) is an independent think tank engaged in action-oriented research to support and influence policy-makers.[10] Located in Dhaka, the Bangladesh Enterprise Institute (BEI) is a non-profit, non-political, research and advocacy think tank established in October 2000. Directed by Farooq Sobhan, a former Foreign Secretary and Ambassador , BEI also serves as a platform to bring the specialist counter terrorism agencies and other security stakeholders together.[11] Similarly, the Bangladesh Institute of Peace and Security Studies (BIPSS) is also a non-profit, non-political, research and advocacy think tank devoted to the study of peace and security issues related to Asia and beyond.[12] Directed by Major General (Retired) Muniruzzaman, BIPSS launched the Bangladesh Centre for Terrorism Research (BCTR) - a specialised centre dedicated to the study, data management and research on terrorism and extremism.

The Institute of International Peace Building (IIPB: Yayasan Prasasti Perdamaian) in Jakarta is a non-profit, non-governmental organisation established in early 2008.[13] It is led by a former journalist Noor Huda Ismail who was a student analyst with ICPVTR in 2006 and holds a master's degree from St Andrews University. A former student of the Jemaah Islamiyah leader Abu Bakar Ba'asyir at the Pondok Pesantren Al Mukmin Ngruki, Huda engaged in de-radicalising former members of Jemaah Islamiyah and other violent extremists. IIPB also conducts extensive field research. The Philippine Institute for Political Violence and Terrorism Research (PIPVTR) is an independent, non-profit, non-governmental organisation launched on March 6, 2008. Renamed the Philippine Institute for Peace, Violence and Terrorism Research, PIPVTR is led by Rommel Banlaoi.

With its origins in November 2007, the Center on Global Counterterrorism Cooperation (GCTC) builds partnerships through collaborative research and policy analysis and by providing practical advice.[14] The Foundation for Defense of Democracies (FDD) launched the Center

[10] Centre for Conflict and Peace Studies, <http://www.caps.af/>, <Accessed August 27, 2012>

[11] Bangladesh Enterprise Institute, <http://www.bei-bd.org/about-bei.php>, <Accessed August 27, 2012>

[12] Bangladesh Institute of Peace and Security Studies, , <http://bipss.org.bd/index.php/page/about-bipss>, <Accessed August 27, 2012>

[13] Yayasan Prasati Perdamaian, <http://www.prasastiperdamaian.com/about/vision-and-mission/>, <Accessed August 27, 2012>

[14] Center on Global Counterterrorism Cooperation, <http://www.globalct.org/about_background.php>, <Accessed August 28, 2012>

for the Study of Terrorist Radicalisation (CSTR) in 2010. The Jamestown Foundation has emerged as a leading provider of research and analysis on conflict and instability in Eurasia. Since its foundation in 1984 as a platform to support Soviet dissidents, The Jamestown Foundation in Washington DC has been regarded for its expertise on terrorism and extremism in Eurasia.[15] One of the best resources to counter-extremism is The Middle East Media Research Institute (MEMRI) in Washington DC. Created in February 1998, MEMRI extensively translates literature produced by terrorist and extremist groups in Arabic, Persian, Urdu-Pashtu and Turkish media into English.[16] Located in DC, MEMRI also has branch offices overseas.[17]

In the UK, in addition to the British government, charities also support several think tanks. Specialist think tanks such as the Quilliam Foundation, which is staffed by former extremists and terrorists, have been effective in countering extremism. Created by Ed Husain, Maajid Nawaz and Rashad Zaman Ali in 2008, Quilliam Foundation is the "world's first counter-extremism think tank set up to address the unique challenges of citizenship, identity, and belonging in a globalised world."[18]

There are a number of foreign ministry and defence ministry research institutes with specialist programs on terrorism studies. The US has regional centres worldwide. One of the best specialist centres is Norwegian Defence Research Establishment's (Forsvarets Forskningsinstitutt – FFI) Terrorism Research Group (TERRA). TERRA conducts research on transnational militant Islamism for the Norwegian Government but publishes many of its products.[19] The Ministry of Foreign Affairs, Malaysia, created its specialist counter terrorism research centre, Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) on July 1, 2003. Based in Kuala Lumpur, SEARCCT engages in research, training and publications.[20]

Many security think tanks with counter terrorism specialists run terrorism research programmes. They mostly consult with governments and

[15] The Jamestown Foundation, <http://www.jamestown.org>,<Accessed August 28, 2012>

[16] The Middle East Media Research Institute, <http://www.memri.org>, <Accessed August 28, 2012>

[17] The Middle East Media Research Institute, <http://www.memri.org/content/en/about.htm>,<Accessed August , 2012>

[18] Quilliam Foundation, < http://www.quilliamfoundation.org/about/>, <Accessed August 28, 2012>

[19] Norwegian Defence Research Establishment, <http://www.ffi.no/en/Terra/Sider/default.aspx> ,<Accessed August 28, 2012>

[20] Southeast Asia Regional Centre for Counter-Terrorism < http://www.searcct.gov.my/>,<Accessed August 28, 2012>

corporations, host seminars and conferences and engage in research and training. Founded in 2003, the George Washington University Homeland Security Policy Institute (HSPI) is a non-partisan "think and do" tank.[21] Led by Frank J. Cilluffo, HSPI builds bridges between theory and practice to advance homeland security through an interdisciplinary approach.[22]

The Washington Institute for Near East Policy produces timely reports on terrorist threats and invites terrorism specialists from around the world to participate in their activities. Former FBI Agent, Matthew Levitt, directs the Stein Program on Counterterrorism and Intelligence at the Institute.[23] Similarly, the long standing Center for Strategic and International Studies (CSIS) in Washington D.C., which is staffed by Arnaud de Borchgrave, Thomas M. Sanderson and Juan Zarate, consults with the government, runs projects and hosts conferences.[24] The Council on Foreign Relations (CFR) has also launched a programme to counter extremism through civil society.[25]

The Against Violent Extremism Network (AVE) was seeded and launched by Google Ideas at the Summit Against Violent Extremism in Dublin in June 2011.[26] Led by Jared Cohen, Director Google Ideas, the Summit brought together former extremists, terrorists and insurgents. Many European counter terrorism academics and practitioners serve in universities and think tanks but there are only a handful of specialist counter terrorism think tanks in most European countries. The Program on Global Terrorism at the Elcano Royal Institute for International and Strategic Studies in Spain led by Professor Fernando Reinares is one such.

Some think tanks lack in-house speciality in countering violent extremism. Such think tanks then invite specialists and convene meetings to

[21] The George Washington University Homeland Security Policy Institute, <http://www.gwumc.edu/hspi/about/mission.cfm> , <Accessed August 28, 2012>

[22] The George Washington University Homeland Security Policy Institute, <http://www.gwumc.edu/hspi/experts/hspiStaff.cfm>, <Accessed August 28, 2012>

[23]The Washington Institute for Near East Policy, < http://www.washingtoninstitute.org/about/research-programs/stein-program-on-counterterrorism-and-intelligence/> , <Accessed August 28, 2012>

[24] Center for Strategic and International Studies, <http://csis.org/category/topics/defense-and-security/terrorism>,<Accessed August 28, 2012>

[25] Council on Foreign Relations, <http://www.cfr.org/thinktank/csmd/>, <Accessed August 28, 2012>

[26] Google Public Policy Blog, <http://googlepublicpolicy.blogspot.sg/2011/06/google-ideas-launches-summit-against.html>, <Accessed August 28, 2012>

discuss the threat of violent extremism. For example, The Chatham House,[27] The International Institute for Strategic Studies,[28] The Ditchely Foundation,[29] Wilton Park[30] and other similar organisations address topical security issues including terrorism and counter terrorism. They generate discussions with the intention of addressing global, regional and national challenges.

Private companies such as the Terrorism Research Center, Soufan Group,[31] Search for International Terrorist Entities (SITE Institute),[32] Stratfor,[33] and World-Check also conduct research and host conferences on terrorism and counter terrorism issues.

In the Middle East, several think tanks work on security measures in collaboration with research programmes on terrorism and extremism. However, with the exception of Israel and Turkey, there are no dedicated think tanks focusing on terrorism in the Middle East. The International Center for Terrorism and Transnational Crime (UTSAM, Uluslararası Terörizm ve Sınıraşan Suçlar Araştırma Merkezi) was established in July 2007. The Centre of Excellence Defence Against Terrorism (Terörizmle Mücadele Mükemmeliyet Merkezi: COE-DAT) was established in Turkey on December 1, 2003.[34] Located in Ankara, Turkey, this NATO- supported think tank engages in training throughout the year.

The leading think tank in the world countering on-line violent extremism is Assakina Campaign for Dialogue. A specialised campaign in the Arabic medium, Assakina not only counters extremism but also promotes moderation by targeting websites, forums and groups. The campaign is spearheaded by Sheikh Ahmad Mun'am al-Mushawwah.

Although there are government think tanks working on terrorism in the Middle East, there are no dedicated academic think tanks working on counter-extremism. The first such think tank will be the International Centre of Excellence for Countering Violent Extremism in Abu Dhabi to be launched in October 2012.

[27] Chatham House, <http://www.chathamhouse.org/research/security>, <Accessed August 28, 2012>

[28] The International Institute for Strategic Studies, <http://www.iiss.org/programmes/transnational-threats-and-political-risk/> , <Accessed August 28, 2012>

[29] The Ditchley Foundation, <http://www.ditchley.co.uk/> , <Accessed August 28, 2012>

[30] Wilton Park, < http://www.wiltonpark.org.uk/en/about-wilton-park/> , <Accessed August 28, 2012>

[31] The Soufan Group, <http://soufangroup.com/>, <Accessed August 28, 2012>

[32] Search for International Terrorist Entities, <http://news.siteintelgroup.com/> , <Accessed August 28, 2012>

[33] Stratfor, < http://www.stratfor.com/about>, <Accessed August 28, 2012>

[34] Centre for Excellence Defence Against Terrorism, <http://www.coedat.nato.int/history.htm>, <Accessed August 28, 2012>

While a variety of US based think tanks do work on threats in Latin America, there are specialised think tanks on Latin American soil dedicated to countering violent extremism. Many experts on Latin American threat groups work for government think tanks and universities.

While there are no dedicated African think tanks engaged in counter extremism, there are a dozen think tanks working on security in general that cover counter terrorism, counter extremism and peace building. They include the Observatory of Conflict and Violence Prevention (OCVP), University of Hargeisa, Somaliland,[35] Center on Global Counterterrorism Cooperation, Ethiopia, African Centre for Security and Strategic Studies, Kenya,[36] Africa Peace and Security Program, Institute for Peace and Security Studies, Addis Ababa University,[37] Africa Center for Strategic Studies, Ethiopia,[38] Institute for Security Studies, South Africa,[39] African Centre for the Constructive Resolution of Disputes (ACCORD), South Africa,[40] and Kenya Muslim Youth Alliance (KMYA).[41]

In the global south, especially in the Muslim world, a few hundred entities engage in countering violent extremism. As they work at the grass root levels, they do not bear the name "counter terrorism" but their work does help to reduce terrorist threat. While some of these think tanks are affiliated to academic or government institutions, others are registered as voluntary and non-governmental entities. These think tanks play activist roles at grass root levels seeking to influence the human terrain. Most of the counter-extremism works conducted by NGO think tanks are project -based. Depending on the funding received from governments or other private donors, they launch initiatives in counter-extremism. The US, Canada, Europe, Australia and Japan through their diplomatic missions provide funding to these NGO think tanks.

Changing Roles of Think Tanks

[35] Observatory of Conflict and Violence Prevention, <http://www.ocvp.org/>, <Accessed August 28, 2012>

[36] African Centre for Security and Strategic Studies, <http://www.afcesss.org> , <Accessed August 28, 2012>

[37] Institute for Peace and Security Studies, <http://www.ipss-addis.org/>, <Accessed August 28, 2012>

[38] Africa Center for Strategic Studies, <http://africacenter.org/> , <Accessed August 28, 2012>

[39] Institute for Security Studies, http://www.issafrica.org/default.php, <Accessed August 29, 2012>

[40] African Centre for the Constructive Resolution of Disputes, http://www.accord.org.za/, <Accessed August 29, 2012>

[41] Kenya Muslim Youth Alliance, <http://kmya.org/>, <Accessed August 28, 2012>

While several hundred think tanks research and publish on terrorism and counter terrorism, the specialist centers focusing exclusively on terrorism studies are less than 100. Of the specialist centres dedicated to the field, a few dozen think tanks use that knowledge to train a new generation of practitioners and scholars. Of the dedicated think tanks working on terrorism and counter terrorism issues, only a few dozen offer university degrees specialising in terrorism studies as most think tanks are without teaching components. Of the university think tanks with research and teaching capabilities, a handful conduct networking and outreach activities in their communities.

Non- university think tanks are best suited to engaging in community networking and outreach activities in many countries suffering from terrorism and extremism. One of the most notable trends is that university think tanks are increasingly working and supporting NGO think tanks engaged in community networking for research and outreach activities to influence the community against ideological extremism and terrorism. Think tanks in the global south working on terrorism studies that have significant language capabilities are also able to conduct research into counter-ideology. Identified as radicalisation studies, these think tanks research and propose recommendations to counter the threat before it matures into terrorism. In future, think tanks working to counter violent extremism must focus on three core areas:

i. Improving Engagement
ii. Capacity Building
iii. Establishing Partnerships[42]

To improve engagement, think tanks must be willing to be inclusive in their approach towards combating violent extremism. Rather than doing research and promoting advocacy at government level to fight violent extremism, there must be an effort to work with the community at large with the aim of developing a comprehensive government-community strategy to mitigate the issues of violent extremism. To stay globally competitive in combating violent extremism and to create an impact, think tanks must also establish partnerships with a variety of stakeholders.

[42] Interview, Salim bin Mohamed Nasir, Associate Research Fellow, International Centre for Political Violence and Terrorism Research, Singapore, August 1, 2012

Security think tanks focusing on terrorism and insurgency were pioneered in the West. Until 9/11, most of the staff who worked and students who trained in these think tanks were Americans, Europeans and Australians. The number of Asians, Africans and Middle Easterners were a handful. With the rise of global terrorism and the proliferation of centers in the West after 9/11, the doors opened for both staff and students from the global south. The decade that followed 9/11 witnessed the emergence of similar academic centres and think tanks worldwide. Until then there was no support in the developing world to create specialist centres working on terrorism and counter terrorism. Most scholars and practitioners viewed the subject of security as the preserve of the government. Although the think tanks in the West experienced terrorism and focused on counter terrorism, their counterparts in the global south better understood radicalisation and focused on counter-radicalisation.

Even as the British launched its counter terrorism strategy CONTEST with Prevent as a strand in early 2003, the West, in general, woke up too late to the challenge of prevention and rehabilitation. With a few exceptions such as the Muslim Contact Unit led by Robert Lambert, Western governments and their partners failed to engage Muslims until the attacks in London on July 7, 2005.[43] The US had no lead agency to counter ideological extremism. Americans committed to freedom of expression were against influencing the beliefs of fellow Americans. Most American scholars and practitioners believed that there was no problem of radicalisation in the US. Under the leadership of David Cohen, the Deputy Commissioner for Intelligence, the New York City Police Department (NYPD) released a study of domestic radicalisation in 2007.[44] Raymond Kelly, the Commissioner, and Cohen were committed to developing a community engagement program but there was no mainstream support. The FBI, too, produced a similar study widely circulated within the law enforcement community. In August 2011, the Obama Administration finally announced its counter-radicalisation strategy. It was devised to address the forces that influenced some people living in the United States to acquire and hold radical or extremist beliefs that may eventually compel them to commit terrorism. This is the first such strategy

[43] Robert Lambert, "Partnering With the Muslim Community as an Effective Counter-Terrorist Strategy," Chatham House, September 21, 2011

[44] Mitchell D. Silber and Arvin Bhatt, Radicalization in the West: The Homegrown Threat, City of New York Police Department, Intelligence Division, New York, 2007.

for the federal government, which calls this effort "combating violent extremism" (CVE).[45]

Conclusion

At the end of the Cold War, the world witnessed a shift from traditional military security to non-traditional security. The think tanks rose up to the challenge posed by non-state armed actors. Today, insurgents, terrorists and extremists from ethno-political, politico-religious and left/ right wing ideologies participate, support and advocate violence. To reduce the threat of violence and extremism, the community of security think tanks must conduct in-depth evidence based research. To find solutions to threats, think tanks serve as the ideal platforms as they bring together specialists from diverse disciplines and cultures. The challenge is to reach the widest possible audience and to influence leaders in governments, corporations and the community. Publicly and privately funded, think tank executives and researchers should produce research on real work issues and make the world a better place. As media shapes public opinion, think tanks have a role to engage both the old and new media. The think tank environment and culture enables its operation in high- risk arenas where governments are hesitant or unable to effect desired change.

As no think tank has a monopoly over knowledge, think tanks should also move towards greater collaboration. Think tanks are vital to change and shape the thinking both of government and the general population. To counter violent extremism, academic, government and NGO think tanks should engage a range of actors. Think tanks can operate at a higher strategic level and at the grassroots level. As such, think tanks are premier influencers of government and society. To reach out to the general population, think tanks must collaborate with the media that shape government and public opinion, religious institutions, the educational establishment, NGOs that play an activist role, and community organisations that influence community perceptions. To be effective, think tanks should work with multiple entities. This can only be done if future think tanks recruit both thinkers and doers.

[45] Countering Violent Extremism in the United States
Jerome P. Bjelopera, Specialist in Organized Crime and Terrorism Congressional Research Service, May 31, 2012

DEFINITION AND FRAMEWORK OF CYBER TERRORISM

Zahri Yunos, Rabiah Ahmad and Noor Azwa Azreen Abd Aziz

ABSTRACT

Cyberspace is a virtual place that has become as important as physical space for social, economic and political activities. Many nations in the world are increasing their dependency on cyberspace when they utilise Information and Communications Technology (ICT). In this digital age, the concept of cyber terrorism has emerged that is the use of cyberspace to carry out terrorist activities. Interestingly, there are many concepts of cyber terrorism provided by academics, researchers, policy makers and individuals. This paper proposes a framework describing the core components of cyber terrorism. The framework defines cyber terrorism from six perspectives: Motivation, target, method of attack, domain, action by perpetrator, and impact.

Keywords: *Cyber Terrorism, Cyberspace, ICT, Cyber Terrorism Framework*

Introduction

Cyberspace and the Internet are at the center of modern life and have become an important medium for political, social and economic expression. Many nations all over the world are becoming increasingly dependent on cyberspace as they maximise the use of Information and Communications Technology (ICT). ICT is a double-edged sword. It can be a useful instrument in maintaining law and order in modern day societies. However, at the same time, it also provides opportunities for criminals to exploit. The real threat from cyberspace does not only come from sovereign states but also from others like individuals or organisations.

The Concept of Cyber Terrorism

The term cyber terrorism was first coined in the 1980s by Collin [1]. According to him, the "virtual world" and the "physical world" converge to form the vehicle of cyber terrorism. Collin further clarifies that the virtual world is the place where computer programs function and data moves, whereas the physical world is the place where we live and function. The growing convergence of the physical and virtual worlds is becoming more complex. Nowadays, ICT plays a major role in the convergence of these two worlds.

Denning [2] defines cyber terrorism as unlawful attacks or threats of attack against computers, networks and the information stored therein, when done to intimidate or coerce a government or its people to further their political or social objectives. Denning also clarifies that, "Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructure could be acts of cyber terrorism, depending on their impact. Attacks that disrupt non-essential services, or that are mainly a costly nuisance, would not." The concept of cyber terrorism as defined by Denning consists of several important components. First, it refers to unlawful attacks. Second, the attacks, and threats of attacks against computers, networks and the information stored within them. Third, the purpose of these unlawful attacks is to intimidate or influence a government or society to further their political or social objectives. Fourth, the attacks result in violence against persons or property, or at least cause enough harm to generate fear. Lastly, serious attacks against critical infrastructure could be construed as acts of cyber terrorism.

Likewise, Lewis [3] defines cyber terrorism as the use of computer network tools to shut down critical national infrastructure (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population. Mantel [4] defines cyber terrorism as highly damaging computer attacks by private individuals designed to generate terror and fear to achieve political or social goals. Mshvidobadze [5] defines cyber terrorism as cyber acts designed to foment terror, or demoralise a target population for a perpetrator's specific purpose, most likely involving some kind of attack on critical infrastructure. Cyber terrorism, as its name implies, involves computer technology and means as a weapon or as a target by terrorist groups or agents [6]. In the context of cyber terrorism, the above definitions suggest that civilian populations and the computer systems of critical infrastructure would appear to be attractive targets to cyber terrorists and contribute to the uniqueness of cyber terrorism resulting in direct damage to both.

It can be argued that the term 'cyber terrorism' comprises components of motivation such as political and, social motivation as well as beliefs. For example, Conway [7] argues that, in order to be labeled as cyber terrorism, the attacks must have a terrorist component, resulting in death and/or large scale destruction, and be politically motivated. Pollitt [8] defines cyber terrorism as the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub- national groups or clandestine agents. Czerpak [9] argues that cyber terrorism is a politically driven attack perpetrated by the use of computers and telecommunications capabilities, which lead to death, bodily injury, explosions and severe economic loss. Nagpal [10] defines cyber terrorism as the premeditated use of disruptive activities, or the threat thereof, in cyberspace, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.

The method of attack in cyber terrorism appears to be the use of computer technology. Beggs [11] defines cyber terrorism as the use of ICT to attack and control critical information systems with the intent to cause harm and to spread fear among people, or at least with the anticipation of changing domestic, national, or international events. Similarly, Weimann [12] defines cyber terrorism as the use of computer network tools to harm or shut down critical national infrastructure (such as energy, transportation and government operations). CRS Report for Congress [13] defines cyber terrorism as the use of computer or weapons, or as targets, by politically motivated international, or sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence people, or cause a government to change its policies.

As defined by Denning, the action by a perpetrator involves unlawful attacks against targeted groups. This notion is supported by Ariely [14] who refers to cyber terrorism as the intentional use, or threat of use, without legally recognised authority, of violence, disruption, or interference against cyber systems resulting in death or injury of a person or persons, substantial damage to physical property, civil disorder or significant economic harm. This understanding is in line with a study conducted by Nelson et al. [15] which defined cyber terrorism as the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological.

Cyber terrorism can have a critical impact on its targeted groups by engendering fear, violence, death and destruction. Stohl [16] argues that cyber terrorism includes some form of intimidation, coercion, influence as well as violence. He defines cyber terrorism as the purposeful act or the threat of the act of violence to create fear and/or compliant behavior in a victim and/or audience of the act or threat. In a report to the United Nations' General Assembly's First Committee on Disarmament and International Security, cyber terrorism mentioned as actions conducted via a computer network that could cause violence against, or generate fear among, people or that could lead to serious political or social destruction [17]. This definition is, perhaps, is taken from the US Government's definition of terrorism which includes the term "computer".

Based on the discussion above, it is clear that there is no common agreement on the concept of cyber terrorism internationally and among researchers. While there are many definitions of cyber terrorism, these suggest a trend that requires further analyses [18] [19] [20] [21]. This is evident as the study of this concept has been the focus of many policy-makers and scholars, but their perspectives vary. Due to the multidimensional structures (or components) of cyber terrorism, it can be said that the concept of cyber terrorism is a contested concept whose interpretation varies from party to party. The context of cyber terrorism denotes different understandings and interpretations and therefore, an accurate knowledge of the context of cyber terrorism enhances clarity of intent. Thus, there is a need for a more structured approach in understanding the various components of cyber terrorism.

The Proposed Cyber Terrorism Framework

This paper proposes that the nature of cyber terrorism should be formulated from six perspectives: motivation, target, method of attack, domain, action by perpetrator, and impact (Figure 1). Motivation is about influencing human beings and the decisions they make. Motivational forces behind cyber terrorism are social, political, ideological and economic. With the growing interconnectedness of critical infrastructure on ICT, the selection of a target that allows the maximum level of disruption would significantly influence the terrorists. Cyber terrorists can exploit vulnerabilities over a targeted system through a vast array of intrusive tools and techniques. The method of attack could be through network warfare and psychological operations. Cyberspace is the domain where a terrorist-type attack is conducted with cyber terrorists employing unlawful use of force or unlawful attacks to conduct a premeditated attack. The impact or consequence is high as the cyber attacks are carried out to intimidate or coerce a government or people leading to violence against them or their properties.

The framework suggests that the core components of cyber terrorism constitute the six perspectives as illustrated in Figure 1. In other words, the framework suggests that all attributes (or components) contribute to the decision-making process in order to determine whether someone gets involved in cyber terrorism or not. The authors suggest that all six components of cyber terrorism in this framework are bound together to form the concept of cyber terrorism.

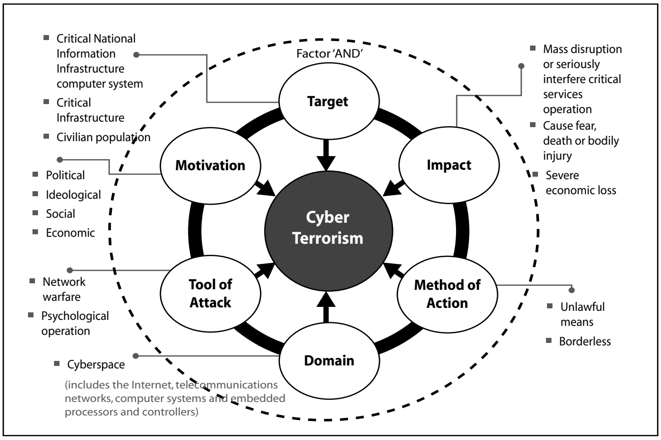
Critical National Information Infrastructure computer system
Critical Infrastructure
Civilian population
Factor 'AND'
Target
Mass disruption or seriously interfere critical services operation
Cause fear, death or bodily injury
Severe economic loss
Motivation
Impact
Political
Ideological
Social
Economic
Cyber Terrorism
Network warfare
Psychological operation
Tool of Attack
Method of Action
Unlawful means
Borderless
Domain
Cyberspace
(includes the Internet, telecommunications networks, computer systems and embedded processors and controllers)

Figure 1: Cyber Terrorism Conceptual Framework

Motivation

Motivation is about influencing human beings and the decisions they make [22]. Perpetrators generally have multiple motives for attacking targets. The motivating forces behind cyber terrorism are political, ideological and social motivation [23]. Through these forces, terrorists are psychologically motivated to drive terrorism. Terrorist intentions are to undermine confidence in the political structure and create difficulty within the body politic. From the motivation perspective, cyber terrorism exists if the person or group of people operates with a specific political or ideological agenda to support their activities [11]. For example, the Irish Republican Army (IRA) engaged in terrorist activities for a predetermined political purpose with the objective of maintaining and strengthening political control [24].

Cyber terrorism can be well understood by identifying the profile of actions or motivations that drive the action of the perpetrators. A politically motivated cyber attack, which results in a tremendous amount of fear and panic among the public, may well be characterised as cyber terrorism even though it does not lead to physical injury or death. Many types of terrorism, including religious terrorism, have strong theological foundations [25]. In the field of cyber terrorism, many look for its causes from the surrounding contexts and underlying conflicts whether social, political or ideological.

Target

The act of cyber terrorism is unique as it combines a specific target with a wider audience [26]. The disruption of the Critical National Information Infrastructure (CNII) would have a severe impact on the economic strength, image, defence and security, public health and safety as well as government capability to function. Based on this argument, the CNII computer system would be an extremely attractive and high-profile target in the world of cyber terrorism [27] and the possibility of disabling the entire CNII communication networks and attacking the civilian community at large would probably be among the most influential factors in a terrorist group's decision, as the damage and destruction would be extraordinarily significant and costly to society and the country attacked.

Due to the advancement of technology, many essential computing services are using the Supervisory Control and Data Acquisition (SCADA) systems, which are connected to the Internet and can be controlled remotely. An attack on the SCADA system that controls and manages critical infrastructure may have been unthinkable in the past, but with current technological developments, it is now possible for the SCADA system to become a target for terrorist attacks. Brunst [28] discusses three scenarios that could be taken into consideration - attacks on hydroelectric dams, tampering with railway and air traffic control systems, and taking over control of power plants. Brunst, in his literature review, provides excellent examples of terrorist attacks in these control systems, which would generate fear within a population. Successful cyber attacks on these control systems would certainly have long-term effects, create fear and pose immediate danger to human lives.

Apart from focusing on the ICT infrastructure, cyber terrorism also targets civilian populations [29] [16] [26]. Attacks against critical infrastructure that spread fear and harm to innocent people within a community would be classified as cyber terrorism [11]. From an effect perspective, consequences on civilian population are immense, thus attracting huge media attention and publicity. The selection of a target that allows the maximum level of disruption would significantly influence the terrorists.

Tools of Attack

Heickero [29] concludes that cyber terrorism comprises different types of methods such as computer network operations and psychological operations. The capability to conduct a cyber attack can be divided into three groups: Simple (unstructured), advanced (structured) and complex (coordinated) [30]. Veerasamy [31] defines network warfare as a modern form of conflict in which computers and networks are used as weapons with information serving as leverage control. Modern forms of network warfare include all the computer and network security means through which computers are attacked and exploited (worms, denial-of-service, bots) as well as all the protective mechanisms being implemented (intrusion detection tools, antivirus software and firewalls).

There has been ample research on individual characteristics, including psychological influences that contribute to a person's motivation for engaging in terrorist activity. Taliharm [32] suggests that the term 'cyber terrorism' should also involve several other activities carried out by terrorists via the Internet, including propaganda via terrorist websites. The dissemination of propaganda via Web 2.0 media is part of the psychological operation [33]. The coverage of mainstream media is important as news coverage in the media is always repeated, thus increasing the reach of the propaganda message.

From a psychological perspective, a disgruntled employee within an organisation also poses a threat to the organisation. However, this category of individuals can be bought; and information can also be sold to terrorist groups. An insider could also act as a cyber terrorist [29]. The extra advantage is that they have inside knowledge. An insider can be planted within the organisation or through a sympathiser who is working in that organisation. The objective is, perhaps, to provide sensitive information or to perform certain tasks such as putting malware into critical control systems for future attacks. In the US, it was reported that 20 employees were arrested for possession of false identification used to obtain security access to facilities containing restricted and sensitive military technology [33].

Domain

Cyber terrorism is the convergence of cyberspace and terrorism. Cyberspace, whether accessed by computer systems or other devices, is the domain (medium) through which a cyber attack would be delivered. The National Security Presidential Directive 54/Homeland Security Presidential Directive 23 of the US Government defines cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers [34]. The UK Government defines cyberspace as an interactive domain that consists of digital networks that are used to store, modify and communicate information. It includes the Internet, but also other information systems that support businesses, infrastructure and services [35].

Cyber terrorism thus can be seen as a relevant threat due to its strong relation to ICT and cyberspace. Apart from land, sea, air and space, cyberspace is another dimension of warfare. Weimann [12] writes that cyberspace is, in many ways, an ideal arena for the activities of extremist terrorist organisations. Among others, it offers an easy and fast flow of information. By its very nature, cyberspace is also capable of reaching out to a vast audience throughout the world by disseminating information in a multimedia environment via the combined use of text, graphics, audio and video.

Method of Action

Rollins and William [33] argue that, there are two views when defining cyber terrorism, which are based on impact (effect-based) and intention (intent-based). They clarify that, effect-based cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals. This implies that, cyber terrorism should focus on the act rather than the perpetrator. Intent-based cyber terrorism, however, exists when "unlawful or politically-motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage".

The cyber terrorist can have the same motives as the traditional terrorist, but they use the computer and network media to attack their targets. [25]. Cyber terrorists use unlawful force or attacks to engage in premeditated attacks to intimidate or coerce a government or people to further their political, social or belief objectives, or to cause severe economic damage. The impact or consequence is high as the attacks are done to intimidate or coerce a government or people and that can lead to violence against persons or properties.

Impact

Cyber terrorism exists when there is an attack on a computer system that leads to violence against a person or property and the disruption is enough to generate fear, death or bodily injury [2] [3]. It is carried out to cause grave harm or severe economic damage or extreme financial harm [24] [13] which could, thus, paralyse world trade and economy. As reported by Rollins and Wilson [33], if terrorists were to launch a widespread cyber attacks, the economy of the country singled out would be the target for disruption, while death and destruction might be considered collateral damage. Terrorist-type cyber attacks may target chemical, biological, radiological or nuclear (CBRN) computer network installations [9] [33]. A successful attack on these installations would cause severe economic disruption and harm to the civilian population in the form of death and bodily injuries.

With the growing interconnectedness and interdependencies of critical infrastructure sectors, cyber terrorism would be directed at those targets that allow for a maximum level of disruption [24] [11]. Terrorists' cyber attacks probably aim at critical infrastructure as their target with successful cyber attacks in one sector having cascading effects on other sectors. Consequently, a large-scale terrorist-type cyber attack could have an unpredictable and, perhaps, catastrophic impact on other sectors, and possibly long-lasting impact on the country's economy.

Conclusion

The term cyber terrorism is becoming increasingly common in popular culture, yet a solid definition of the word seems elusive. There is no universally accepted definition for the word cyber terrorism. Cyber terrorism is about threat perception that makes the concept differ from one to another. The concept of this term is an essentially contested concept where its interpretation differs among academics, researchers, professionals and policy makers.

Due to the trans-boundary nature of cyber terrorism, there needs to exist a mutual understanding between countries about what constitutes cyber terrorism. Understanding the perceptual similarities and differences in cyber terrorism can provide us with an insight into the concept of cyber terrorism. This work provides a baseline in establishing and defining the concept of cyber terrorism. The perspectives are useful in determining whether someone is involved in cyber terrorism or not.

For future works, this framework can be validated and assessed by encompassing both qualitative and quantitative techniques. Quantitative methods can be used to quantify the data with applied statistical methods being used to test the dynamic relationships between the components of the cyber terrorism framework. Additionally, future research from this study could be used to improve the definition of the concept of cyber terrorism and its adoption in a holistic manner. Continued research in this area can be conducted and this may lead to the development of a strategic and technological framework to counter cyber terrorism.

References

[1] B. L. Collin, "The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge," in *11th Annual International Symposium Criminal Justice Issues*, 1996, vol. 93, no. 4.

[2] D. E. Denning, "Cyberterrorism," *Testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism, May 23*, 2000.

[3] J. A. Lewis, "Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats," Center for Strategic and International Studies, 2002.

[4] B. Mantel, "Terrorism and the Internet. Should Web Sites That Promote Terrorism Be Shut Down?," CQ Researcher, pp. 129-152, 2009.

[5] K. Mshvidobadze, "State-sponsored Cyber Terrorism : Georgia's Experience," *Presentation to the Georgian Foundation for Strategic and International Studies*, pp. 1-7, 2011.

[6] S. Krasavin, "What is Cyber-terrorism," *Computer Crime Research Center* (CCRC), 2001. [Online]. Available: www.crime-research.org/library/cyber-terrorism.htm. [Accessed: 09-Jun-2008].

[7] M. Conway, "Reality Bytes : Cyberterrorism and Terrorist 'Use' of the Internet," *FIRST MONDAY, Journal on the Internet*, 2002. [Online]. Available: www.firstmonday.org/ISSUES/issue7_11/conway. [Accessed: 09-Jun-2008].

[8] M. M. Pollitt, "Cyberterrorism — Fact or Fancy?," *Computer Fraud & Security*, no. 2, pp. 8-10, 1998.

[9] P. Czerpak, "The European Dimension of the Flight against Cyber-terrorism – A Theoretical Approach," in *Europe and Complex Security*

Issues, 2005, pp. 309-318.

[10] R. Nagpal, "Cyber Terrorism in the Context of Globalization," in *II World Congress on Informatics and Law*, 2002, no. September, pp. 1-23.

[11] C. Beggs, "Cyber-Terrorism in Australia," *IGI Global*, pp. 108-113, 2008.

[12] G. Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," *United States Institute of Peace*, no. Special Report 116, pp. 1-11, 2004.

[13] C. Wilson, "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," 2005.

[14] G. Ariely, "Knowledge Management, Terrorism and Cyber Terrorism," in *Cyber Warfare and Cyber Terrorism*, L. J. Janczewski and A. M. Corarik, Eds. Hersey, New York: Information Science Reference, 2008.

[15] B. Nelson, R. Choi, M. Iacobucci, M. Mitchell, and G. Gagnon, "Cyberterror: Prospects and Implications." Center for the Study of Terrorism and Irregular Warfare, Montery, CA, 1999.

[16] M. Stohl, "Cyber Terrorism : A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Game?," *Springer Science + Business Media B.V*, pp. 1-16, 2007.

[17] S. T. Dang, "The Prevention of Cyberterrorism and Cyberwar," in *Old Dominion University Model United Nations Conference (ODUMUNC)*, 2011, pp. 1-6.

[18] M. Dogrul, A. Aslan, and E. Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," in *2011 3rd International Conference on Cyber Conflict, Tallinn, Estonia, 7-10 June*, 2011, pp. 1-15.

[19] P. A. H. Williams, "Information Warfare: Time for a Redefinition," in *Proceedings of the 11th Australian Information Warfare & Security Conference, Perth Western, Australia, 30 Nov - 2 Dec*, 2010, pp. 37-44.

[20] C. Czosseck, R. Ottis, and A. M. Taliharm, "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *International Journal of Cyber Warfare and Terrorism*, vol. 1, no. 1, pp. 24-34, 2011.

[21] J. Matusitz, "Social Network Theory: A Comparative Analysis of the Jewish Revolt in Antiquity and the Cyber Terrorism Incident over Kosovo," *Information Security Journal: A Global Perspective*, vol. 20, no. 1, pp. 34-44, Feb. 2011.

[22] N. Veerasamy and J. H. P. Eloff, "Towards a Framework for a Network Warfare Capability," in *Proceedings of the ISSA 2008 Innovative Minds*

Conference, 7-9 Jul, 2008, pp. 405-422.

[23] M. D. Cavelty, "Critical Information Infrastructure: Vulnerabilities, Threats and Responses," *ICTs and International Security*, pp. 15-22, 2007.

[24] P. Flemming and M. Stohl, "Myths and Realities of Cyberterrorism," *Proceeding on Countering Terrorism through Enhanced International Cooperation*, pp. 70-105, 2000.

[25] N. Veerasamy, "Motivation for Cyberterrorism," *9th Annual Information Security South Africa (ISSA) - Towards New Security Paradigms*, p. 6, 2010.

[26] G. Ackerman et al., "Assessing Terrorist Motivations for Attacking Critical Infrastructure," *Center for Nonproliferation Studies, Monterey Institute of International Studies, California*, Jul. 2007.

[27] T. G. Lewis, T. J. Mackin, and R. Darken, "Critical Infrastructure as Complex Emergent Systems," *International Journal of Cyber Warfare & Terrorism*, vol. 1, no. 1, pp. 1-12, 2011.

[28] P. W. Brunst, "Terrorism and the Internet: New Threats Posed by Counterterrorism and Terrorist Use of the Internet," pp. 51-79, 2010.

[29] R. Heickero, "Terrorism Online and the Change of Modus Operandi," *Swedish Defence Research Agency, Stockholm, Sweden*, pp. 1-13, 2007.

[30] T. F. O'Hara, "Cyber Warfare/Cyber Terrorism," *USAWC Strategy Research Project*, 2004.

[31] N. Veerasamy and J. H. P. Eloff, "Application Of Non-Quantitative Modelling In The Analysis Of A Network Warfare Environment," in *World Academy of Science, Engineering and Technology Conference, Paris, France*, 2008.

[32] A. M. Taliharm, "Emerging Security Challenges and Cyber Terrorism," *Digital Development Debates #5 Securing Peace #Future Wars*, 2011. [Online]. Available: http://www.digital-development-debates.org/05-securing-peace/future-wars.html. [Accessed: 19-Mar-2012].

[33] J. Rollins and C. Wilson, "Terrorist Capabilities for Cyberattack: Overview and Policy Issues," CRS Report for Congress, 2007.

[34] United States of America, "Cyberspace Policy Review : Assuring a Trusted and Resilient Information and Communication Infrastructure," 2009. [Online]. Available: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. [Accessed: 19-Mar-2012].

[35] UK Cabinet Office, "The UK Cyber Security Strategy - Protecting and Promoting the UK in a Digital World," 2011. [Online]. Available: http://www.cabinetoffice.gov.uk/sites/default/files/resources/The UK Cyber Security Strategy- web ver.pdf. [Accessed: 19-Mar-2012].

NOTES ON CONTRIBUTORS

Kumar Ramakrishna is an Assosciate Professor and Head of the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS), Singapore. He was Head (Studies) of the School from 2003-2006, He obtained a First Class (Honours) in Political Science from the National University of Singapore in 1989 and a Masters Degree in Defence Studies from University of New South Wales in 1992. He went on to secure his PhD in History from Royal Holloway and Bedford New College, University of London in1999. His current research interest include British propaganda in the Malayan Emergency, propaganda theory and practice, history of strategic thought and counter-terrorism, with a focus on radicalisation. He was also an Australian Department of Foreign Affairs and Trade (DFAT) Special Visitor in March 2003. In 2008, he was appointed Senior Advisor to the Trusted Information Network on Extremism and Transnational Crime in Southeast Asia and Australia. He has co-edited two well-received books on counter-terrorism, *The New Terrorism: Anatomy, Trends and Counter-Strategies* (2002) as well as *After Bali: The Threat of Terrorism in Southeast Asia* (2004). He has also written two books entitled *Emergency Propaganda: The Winning of Malayan Hearts and Minds, 1948-1958* (2002) and *Radical Pathways: Understanding Muslim Radicalisation in Indonesia* (2009). He is a member of the Singapore Government Parliamentary Committee (GPC) Resource Panel on Home Affairs and Law, member of the Board of Trustees, the Institute of Southeast Asian Studies in Singapore, member of the Board of Governors of the Islamic Religious Council of Singapore (MUIS) Academy, and Executive Committee Member of the Political Science Association (Singapore). He is a member of the Executive Board of the Council for Asian Transnational Threats Research.

Nazery Khalid is a Research Fellow at Maritime Institute of Malaysia's (MIMA) Center for Economics Studies & Ocean Industries. He has presented talks and papers at many international conferences and forums on a wide range of maritime issues including port development, maritime security, ship financing, multimodal transport, offshore oil and gas and freight logistics. His research findings and views on various maritime issues are often quoted in the media and have appeared in various publications and maritime journals. Nazery holds a Bachelor of Arts degree in Business Administration from Ottawa University, Kansas, USA and an MBA from International Islamic University, Malaysia.

Nishchal N. Pandey is Director of the Centre for South Asian Studies, Kathmandu and is a well-known Nepali strategic analyst. A man of letter, he is author of three books: "Nepal's Maoist Movement and Implications for India and China" (Manohar, 2005), "India's North-Eastern Region: Insurgency, Economic Development and Linkages with Southeast Asia", (Manohar Publishers, 2008) and "New Nepal: The Fault-lines" (SAGE Publications, 2010). He obtained his PhD. from Tribhuvan University, Kathmandu and was a Visiting Fellow at the Institute of South Asian Studies (ISAS), Singapore in 2006-07 and Visiting Fellow at the University of Hull, UK in 2009. Some of his edited books include: "New Life within SAARC" (IFA, 2005), "Labour Issues and Foreign Policy" (IFA, 2006), "Nepal-Japan Relations" (IFA, 2006), "Nepal as a Transit State: Emerging Possibilities" (IFA, 2006). He is also the Co-Editor of "Comprehensive Security in South Asia" (Manohar Publishers, 2006). His latest co-edited books are: "Nepal's National Interests" (CSAS-KAS, 2011), "Towards a More Cooperative South Asia (CSAS-KAS, 2012) and "SAARC: Towards Meaningful Cooperation" (CSAS-KAS, 2012). He is at present an international research committee member of the Regional Centre for Strategic Studies, Colombo and visiting fellow at the Institute of Peace and Conflict Studies, New Delhi. He was also Advisor to the National Planning Commission of Nepal in 1997. He can be reached at: nina@ntc.net.np.

Noor Azwa Azreen Abd Aziz is currently the Strategic Policy Research Executive at CyberSecurity Malaysia. She holds a Bachelor's Degree in International Relations from Victoria University of Wellington, New Zealand.

Rabiah Ahmad is an Associate Professor at the Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka, Malaysia. She received her PhD in Information Studies (Health Informatics) from the University of Sheffield, UK, and M.Sc. (Information Security) from the Royal Holloway University of London, UK. Her research interests include healthcare system security and information security architecture. She has delivered papers at various health informatics and information security conferences at national as well as international levels. She has also published papers in accredited national/international journals. Besides that, she also serves as a reviewer for various conferences and journals.

Ranga Kalansooriya is a journalist from Sri Lanka has been reporting on his country's conflict to local and international media for over 18 years. He is currently reading for his PhD on reporting ethnicity in the vernacular press. Ranga is a Reuter's Fellow at Oxford University, United Kingdom. His publication 'LTTE and IRA – Combating Terrorism and Discussing Peace' [Case studies, The Northern Ireland and Sri Lankan Peace Processes] was based on his research at Oxford University in 2001. He received his Master's Degree from the Asia-Europe Institute, University of Malaya, Kuala Lumpur and Bachelor of Science (Mathematics) degree from the Open University of Sri Lanka. The Master's Research project on 'e-fying terrorism' was conducted at the Institute of Defence and Strategic Studies at Nanyang Technological University, Singapore.He was appointed spokesman to the Minister of Foreign Affairs, Sri Lanka and then became Counsellor (Information), Sri Lanka High Commission, Kuala Lumpur. He is a visiting Lecturer in Journalism in several Sri Lankan universities. After completing his diploma in News Agency Journalism at the Indian Institute of Mass Communications, New Delhi, Ranga attended Reuters Training on International News Writing, Reuters Headquarters, London and UN training on Reporting UN and International Affairs, UN Headquarters, New York. He is a Member of the Governing Board of the Council for Transnational Threat Research (CATR) established by the Institute of Defence Analysis (IDA) Washington DC. He was also the Director General of the Sri Lanka Press Institute until August 2009 – the managing body of the Sri Lanka College of Journalism and the Press Complaints Commission of Sri Lanka. Currently he is the Asia Pacific Advisor to the International Media Support in Denmark.

Rohan Gunaratna is an Associate Professor and Head of Rajaratnam School of International Studies' (RSIS) International Centre for Political Violence and Terrorism Research (ICPVTR). He obtained his PhD in International Relations from the University of St. Andrews, Scotland and a M.A. in International Peace Studies from the University of Notre Dame. His research areas include terrorist operational and support networks, maritime terrorist tactics, technologies and techniques, terrorist organisations, suicide terrorism, terrorist rehabilitation, counter-terrorism intelligence and terrorism in Asia, Africa and the Middle East. He is also the author and editor of at least 15 books including "Inside Al Qaeda: Global Network of Terror" (Columbia University Press). He is also a member of the Advisory board, International Centre for Counter-Terrorism, The Hague, member of the steering committee of George Washington University's Homeland Security Policy Institute, Senior advisor, CSIS Washington DC Project on Arc of Instability and Project on Al Qaeda and Associated Movements and Senior Fellow Alumnus at the United States Military Academy's Combating Terrorism Centre at West Point. He is also the litigation consultant to the U.S Department of Justice.

Zahri Yunos is currently the Acting Chief Executive Officer of CyberSecurity Malaysia. Zahri holds a Master's degree in Electrical Engineering from the Universiti Teknologi Malaysia, Malaysia and a Bachelor's degree in Computer Science from the Fairleigh Dickinson University, New Jersey, USA. He is a certified Associate Business Continuity Professional by the Disaster Recovery Institute International, USA. Zahri has been awarded Senior Information Security Professional Honoree in July 2010 by the $(ISC)^2$, USA. He has contributed various articles and presented papers on topics related to cyber security and Business Continuity Management.