Special Issue : **Policing Terrorism and Radicalism**

Recognized by
Higher Education Commission (HEC), Pakistan
vide letter No.DD/Jour/SS&H/2012/216

Pakistan Journal of Criminology

Volume 3 / Number 3 / January, 2012

Guest Editor
Dr. Geoff Dean (Australia)

PAKISTAN SOCIETY OF CRIMINOLOGY (PSC)
http://www.pakistansocietyofcriminology.com

Pakistan Journal of Criminology
Volume 3 / Number 3 / January, 2012

Pakistan Journal of Criminology

Volume 3, No. 3, January, 2012

Contents

Causes of Radicalism and Responses in Pakistan
A Note from Editor-in-Chief
Fasihuddin i

Comments from the Guest Editor
Dr. Geoff Dean (Australia) vii

Policing the Perilous Euroland: Countering Terrorism and Radicalization in Europe
Monica den Boer & Irene Wiegand 1

Social Network Analysis of Terrorist Networks: Can it add value?
Mark Lauchs, Robyn Keast and Vy Le 21

Assessing Terrorist Risks: Developing an Algorithm-Based Model for Law Enforcement
Frederic Lemieux and Regens, 33

Terrorism Investigations in Pakistan: Current Perceptions and Realities of Frontline Police
Fasihuddin 51

Are Suicide Bombers Coming from Madaris (Islamic Schools) in Pakistan?
Fasihuddin and Imran Ahmad Sajid 79

The Dark Side of Social Media: Review of Online Terrorism
Geoff Dean, Peter Bell, Jack Newman 107

Contents

The Challenge of Cyber Crime in India: The Role of Government
Atul Bamrara 127

Book Review
Sujit Das, Blasphemous Book: The Fallacies of Sujit Das
Imran Ahmad Sajid 135

Community Engagement 139

Visit: http://www.pakistansocietyofcriminology.com
Email:pscatpeshawar@yahoo.com
pscatcriminology@gmail.com
Free access to tables of contents and abstracts.

Causes of Radicalism and Responses in Pakistan
A Note from Editor-in-Chief

Radicalism and terrorism have become synonymous in the context of Pakistan as is evident from numerous reports, books and articles written on the causes, processes, dynamics and responses of terrorism, militancy, radicalism and *Jihad.* The people of Pakistan don't approve of many of the misnomers and propagandist words like Islamic radicalism, global jihadism, and so forth. Many such ill-informed terms derive from the ignorance and simplicity of the Western media and naive journalists or far-removed scholars who have no direct access to, or comprehensive knowledge of, true Islamic literature. Tragically, Pakistan is dubbed today as the hub of these militant and radical elements that stretch back in people's minds to the horrific images of 9/11. US Defence Secretary Robert Gates described western Pakistan as '*the greatest threat to the homeland*' in Sept, 2008. In the same month Admiral Mike Mullen stated that 'Pakistan is not another country but a country with a growing insurgency, with a border that's a safe haven for militants who pose America's *toughest national security problem*'[1].

In tracing back the real underlying causes of this threatening militancy, non-accommodation, violence, radical ideas, and resultant terrorism incidents, many have put the burden on the history of Islam and the Indian sub-continent. This includes the pre-independence communalism (Hindu-Muslim tensions in India before 1947); anti-ahmadi campaigns of the 1950s; the Afghan-Soviet Jihad and the current rising anti-Americanism after the war on terror since 2001[2]. In addition to these historic drivers and their unstoppable implications, scholars describe a list of facilitating factors which further nurture the feelings and environment of radicalism and intolerance. Such factors like identity crisis; enhanced provincial; ethnic and sectarian strife in Pakistani society; lack of viable democratic forums; and abysmally low human development, especially in the areas which are easily infiltrated and insinuated by non-state actors, and more importantly by disgruntled political and religious elements.[3] Some authors more specifically point at the chronic poverty, primitive tribal culture, ungoverned areas and intense military operations in Pakistan's tribal belt as another set of facilitating factors for growing radicalism.[4] The US/Nato air-strikes against Al-Qaeda's top leadership and the concomitant civilian casualties are often counter-productive and rarely of any help in reducing radicalism.[5] This 'will-o-the-wisp' chase of locating the precise root-causes of radicalism has often targeted the Islamic seminaries (*Madrassahs*) as potential places for breeding terrorists and radicals.[6] Copious literature has come out on this Madrassahs-militancy connection, but rarely has any significant empirical research been done to prove this assumed ' connection' beyond doubt. In fact, like

much so-called 'supporting evidence' about radicalization, the view that madrassahs are hotbeds of militancy with the implied connection about the influence of Islamic schools is far from clear-cut. Silke (2008:110) quotes research by Sageman (2004) that "found only 18 percent of Islamist extremists have had an Islamic religious primary or secondary education. In contrast, 82 percent went to secular schools." Hence, Silke (op.cit) argues that "These data undermine the view that Islamic extremism can be best viewed as resulting from brainwashing by teachers in madrassas as part of normal primary or secondary education."

From here the discussion on root-causes of radicalism gets irrationally extended to the religion of Islam. Combine this hyper-emotionalism about Islamic religion with certain unfavourable phenomena like Danish cartoons, sacrilege desecration of the Holy Book and other unkind and unreasonable bashing of religious emblems, it is little wonder serious violence get triggered. Thus a vicious cycle of further intensified relations between the West and the Muslim world globally is set in motion and also between the liberals/moderates and orthodox within Muslim societies. These actions and reactions diverted the attention of some into far-fetched areas looking for justifications. For instance, some writers have started looking the causes of militancy in centuries-old Muslim writers and scholars like Ibn-Taymiah,[7] who, if living in this era, would have probably said something different. Such accounts of centuries old writers like Ibn-Taymiah or Shaikh Abdul Wahab can become an ill-fated academic exercise in re-inventing history in one' preferred image which ignores the environment of that time and its geo-political dictates and the compulsions in the Muslim world in an era that saw its declining civilization.

Some local researches, based on public perception, though indigenous but limited in nature, have found Afghan conflict, extreme poverty, unemployment and bad governance as the causes and facilitating factors of radicalism in the Federally Administered Tribal Areas (FATA) of Pakistan.[8] Some found the desire of the militants or Jihadi groups as a root cause to establish a global new Muslim world order in order to restore the glory of Islam.[9] However, many moderate Muslim thinkers, like Allama Wahiduddin Khan, oppose this view vehemently and attribute the Muslim glory of the past to the remarkable educational and scientific achievements of the medieval Muslims when the West was passing through its dark ages, and not to the political dominance of the Muslim caliphate.[10] The Allama also attributes the current dominance of the Western civilization to its advancement in physical and social sciences rather than to its wars, political interventions and alliances. This debate on the revivalism of Muslim glory has given ample pretext, throughout history, to various international powers and intellectuals to keep their assets in this part of the world, especially the under-developed tribal regions in

which otherwise can't be generalized to the public at large. The 'problem-tree analysis' technique has still not satisfied the researchers and criminologists on the exact nature, extent, pattern and magnitude of the causes and facilitating factors of radicalism in Pakistan's society.

On the other hand, some of Muslim scholars have also tried to identify the 'real' causative agents of intolerance and radicalism, and have enumerated a long list of reasons. For example, the mutual accusations of Muslim sects; decrying one another as non-believers; the jihadi culture; the abundance of arms and drugs after the Afghan-Soviet war; the mis-use of religion; ignorance; illiteracy; poverty; unemployment; colossal foreign aid; the absence of spiritualism; and more violence in the garb of eradicating violence[11] as the real causes of radicalism. Some religious scholars have outspokenly blamed the separation of religion and politics, feudalism, class struggle and conflicting educational systems in the country as the true causes of religious intolerance and radicalism.[12] The debate will continue between the various schools of thought and more interesting observations will come out which will generate more debate for further research and analysis on how to fix the issue and how to develop workable solutions for some of these corresponding responses to the true causes.

This task will not be easy or quick. It is clearly evident from this brief overview of the search for root causes and facilitating factors that drives radicalism, that there is little empirical research to back up claims and counter claims. So many claims are based on theoretical research, analyses, speculations or personal accounts, which undoubtedly are amenable and susceptible to personal biases of one or another group. To further confound an already messy whirlpool of conjectures, the study of terrorism in most Western countries sits under the disciplinary banner of political science. A 'science' noted more for polemic debates and political intrigues than its science.

As the above discussion suggests we can't identify one single cause for the highly complex phenomenon of radicalism. Similarly, is the case for the plethora of responses, like the vague 3D policy of Pakistan—the deterrence, dialogue and development—as a counter-terror policy. However no one knows the details of any D of these three. Pakistan still has no proper policy on de-radicalization which can satisfactorily address the problems of FATA development, tribal community engagement, youth unemployment, effective community and intelligence-led policing in urban and rural areas, educational reforms and especially standardization of religious education and literature, police reforms directing at police specialization and training, and the effective use of civil society and the media for messaging of the anti-radical slogans and concepts, to name a few. Furthermore, the uneven development and conflicting ideologies spread by diverse educational

systems needs to be rectified between the opposing segments of Pakistan society. Moreover, the administrative breakdown in certain terror-affected areas needs to be administered with local and traditional mechanisms of conflict-resolution like mediation, arbitration and local assemblies (*Jirgas*). All these steps need proper legal protection, legitimacy and resource allocations with able minded, creative and committed officers. The ad-hoc arrangements like raising armed bands (*lashkars*) may be counter-productive and may add further bloodshed in a revenge-based tribal society. Wishful mega ideas like that of creating new provinces or merging FATA with one or another province will simply add to and augment the bundles of serious administrative problems. At the moment, we need a few small confidence-building measures in FATA and Baluchistan in particular, before any 'mega' intervention is likely to succeed in the already poverty-stricken, terror-hit and constantly ignored areas of Pakistan.

Finally, I am extremely thankful to the Guest-Editor, who very kindly edited this special issue of *Pakistan Journal of Criminology.* As this special issue demonstrates the PJC is continuously moving in the direction of introducing authentic criminological literature to the body of social sciences in Pakistan. Also, the Pakistan Society of Criminology is indebted to the AUSAID/Australian Federal Police (AFP) for providing funds for the publication and printing of this special issue, though AUSAID and AFP have no responsibility for its contents. Certainly this special issue will be of immense interest to the local police and law-enforcement agencies in Pakistan for their guidance on policing terrorism and radicalism in the light of available criminological scholarship and international best practices.

It is also to be announced with immense pleasure that the Higher Education Commission of Pakistan has recognized the Pakistan Journal of Criminology which is a great achievement of criminology in Pakistan. All the members of the Editorial and Advisory Boards and well-wishers of PJC and Pakistan Society of Criminology deserve our profound congratulation and thanks.

Fasihuddin (PSP)
Editor - in - Chief
email: fasih68@hotmail.com

End Notes

[1]Fasihuddin. (2011). Causes of Radicalism: Policing Terrorism in Pakistan. Paper presented at the University of Huddersfield, UK on 20 June, 2011.

[2]Sana Haroon. (2008). The Rise of Deobandi Islam in NWFP and its Implications in Colonial India and Pakistan, 1914-1996. In *Journal of Asiatic Society.* see also Sana Haroon. (2007). *The Frontier of Faith: : Islam in the Indo-Afghan Borderland*. Karachi: Oxford University Press.

[3]Joshua T. White. (2008). *Pakistan's Islamist Frontier: Islamic Politics and U.S. Policy in Pakistan's North-West Frontier*. In, Religion & Security Monograph Series, no. 1. Arlington, VA: Center on Faith & International Affairs; see also Stephen P. Cohen. (2004). *The Idea of Pakistan*. Washington DC: Brookings Institution Press; see also *The Militant Jihadi Challenges*. (2009). The International Crisis Group Report on Pakistan. Retrieved Jan 5, 2012 from http://www.crisisgroup.org/en/regions/asia/south-asia/pakistan.aspx

[4]See Thomas H. Johnson & M. Chris Mason. (2008). No Sign Until the Burst of Fire: Understanding Pakistan-Afghanistan Frontier. In *Journal of International Security*, volume 32, issue 4, pages 41-77. Spring.

[5]Laila Bokhari. (2011). Radicalization, Political Violence, and Militancy. In Stephen P. Coehen. *The Future of Pakistan*. Islamabad: Vanguard Books.

[6]Ekaterina Stepanova. (2008). *Terrorism in Asymmetrical Conflict Ideological and Structural Aspects.* SIPRI Research Report No. 23. Stockholm International Peace Research Institute. Retrieved Jan 1, 2012 from http://books.sipri.org/files/RR/SIPRIRR23.pdf

[7]Sleem Shehzad. (2001).*Inside Al-Qaeda and the Taliban: Beyond Bin Laden and 9/11*. London: Pluto Press.

[8]Naveed Ahmad Shinwari. (2011). *Understanding FATA: Attitude towards Governance, Religion & Pakistan's Federally Administered Tribal Areas*. Volume IV. Islamabad: CAMP.

[9]Sohail Abbas. (2007). *Probing the Jihadi Mindset.* Islamabad: Millat Publications; see also the website http://www.khilafah.com/ which is promoting Khilafah movement globally.

[10]Fasihuddin. (Tuesday, June 28, 2011). *Amrici Dushmani aur Allama Wahiduddin Khan kay Afkar* [Urdu]. Anti-Americanism and views of Allama Wahiddudin Khan. In Daily *Aaj*. Peshawar: Retrieved Jan 1, 2012 from http://www.dailyaaj.com.pk/?p=20554

[11]Dr. Muhammad Humayun Abbas Shams. (2006). *Mazhabi Intiha-Pasandi aur Uska Tadaruk Taleemat-i-Nabvi ki Roshni Main*. [Urdu]. Religious Intolerance and its Prevention in Light of the Teachings of the Holy Prophet (PBUH). Lahore: Jamal-i-Karam Publications.

[12]See Monthly *Tajziat*, Issue 31-33 (July-Sept, 2011), Islamabad.

For further reading please see

Dr. Israr Ahmad. (1997). *Jihad-bil-Quran* [Urdu]. Lahore: Maktaba Khuddam ul Quran Publishers;

Dr. Israr Ahmad. (1999). *Jihad Fi-Sabeelilllah*. [Urdu]. Lahore: Maktaba Khuddam ul Quran Publishers;

Maulana Abul Ala Maodudi. (1988). *Al-Jihad-fil-Islam*. Lahore. Idara Tarjumanul Quran Publishers;

Maulana Wahiduddin Khan. (2002). *True Meaning of Jihad: The Concepts of Peace, Tolerance and Non-Violence in Islam*. Retrieved Jan 1, 2012 from http://cpsglobal.org/content/true-jihad-0 ; and

Brian M. Jenkins, et. al. (2007). *Terrorism: What's Coming The Mutating Threat*. Oklahoma, USA: Memorial Institute for the Prevention of Terrorism.

Peter R. Neumann (2010). *Prisons and Terrorism, Radicalisation and De-Redicalisation in 15 Countries* (Report), The International Centre For The Study of Radicalisation and Political Violence (ICSR), www.icscr.info

Andrew Silke (2008). "Holy Warriors: Exploring the Psychological Processes of Jihadi Radicalization". *European Journal of Criminology*. *5(1): 99-123.* Accessed 8 August, 2011.
http://euc.sagepub.com.ezp01.library.qut.edu.au/content/5/1/99.full.pdf+html

Comments from the Guest Editor

This Special Issue on 'Policing Terrorism and Radicalism' for the Pakistan Journal of Criminology brings together a wide and diverse range of researchers, academics and practitioners from around the world. This Special Issue contains a balanced mix of theory and practice that will resonate with anyone wanting to know and learn more about the complexities which underpin the twin brothers of terrorism and radicalism. The diversity of the articles is such that I have thematically arranged them, somewhat loosely; around three key notions associated with policing terrorism and radicalism – namely, a*ssessment, cyber space* and *investigations*.

The first three articles deal with the theme of *assessment* firstly through the wide lens of policy in relation to counter terrorism, then in terms of the value that social network analysis holds for understanding terrorist networks, and finally how best to go about assessing terrorist risks. The trauma of 9/11 propelled the issue terrorism onto the policy agenda of many countries worldwide. The first article deals with the European response to countering terrorism and radicalization at the policy level. In den Boer and Wiegand's article they discuss how the EU has sought to enlist the cooperation of number states through a three-pronged policy of strategic, regulatory and agency cooperation. Their analysis reveals that counter-terrorism policy in the EU has become an irreversible process of strategic and legislative harmonization which will continue well into the future.

The second article related to the theme of assessment presents a cogent argument about the value that Social Network Analysis (SNA) has for understanding how terrorist groups form and operate. SNA allows the 'hidden' or opaque structure and relations of terrorist networks to become more visible and, therefore, open to intervention. The authors make the point that SNA helps attack the resilience of groups by identifying membership links, money movements and information flows within a network. Metrics provide a way to assess the strengths and weaknesses of a network and hence allow targeting of individuals whose removal will most effectively disrupt the terrorist group's operations. Furthermore, the authors assert that whilst academics are unlikely to be studying real-time information in the same manner as intelligence agencies, they still can make a valuable contribution by developing theories and conceptual frameworks about terrorist group structures and operations which will allow law enforcement practitioners to better understand and target terrorist group vulnerabilities and longevity.

The third article outlines the basic principles of a risk-based approach to strategic terrorism threat assessment. Lemieux and Regens make a noteworthy contribution by not only presenting a comprehensive critic of existing terrorism

threat assessment models but also by proposing an intriguing alternative logic model based on several factors related to the threat, vulnerability and uncertainty of terrorist attacks. These authors argue that the application of algorithm model, like the one they outline, to terrorism risk assessment can help to better understand the patterns of violent groups over a period of time. This approach can serve both operational and strategic purposes by providing realistic measures to investigators and intelligence officers on threat and vulnerability characteristics and using individual terrorism group risk factors to help decision-makers to identify strategic priorities as well as appropriate tactics to reduce vulnerabilities and mitigate threats. The authors to their credit point also out that like all conceptual frameworks and theoretical models there are limitations inherent in any design. Their model is not a 'crystal ball' that can predict terrorist attacks. Also, it requires the availability of significant amounts of data in order to generate reliable models. However, this algorithm-based application is a robust risk analysis tool that can assist law enforcement agencies to prioritize groups that present the most serious security risks, allocate resource efficiently, and elaborate more effective counter-terrorism strategies and tactics.

The second theme deals with the nature of *investigations* regarding terrorism cases. The first of two articles under this investigative theme, presents a sober analysis of the multiplicity of constraints faced by frontline police in Pakistan when undertaking investigations into terrorism cases. In this article, Fasihuddin has undertaken groundbreaking research that presents an extremely depressing picture of how burdened down terrorism investigations are in Pakistan, particularly in the KPK province. The findings document the poor quality of investigation management that result in low arrest rates and mismanaged prosecutions. The complexity of this issue is further compounded by a serious lack of empirical research on terrorism investigations and its management in Pakistan and the absence of a meaningful and effective counter-terrorism policy at the national level. As the author states “Pakistan's policy-makers terribly failed to create a consensus on a national strategy”. Such a policy vacuum in Pakistan is in stark contrast to what has occurred in the EU and its counter-terrorism policy of strategic, agency and legislative harmonization as noted in the first article by den Boer and Wiegand.

The next article related to the theme of investigation, posed a vexing question, “Are Suicide Bombers Coming from Madaris (Islamic Schools) in Pakistan?” The authors, Fasihuddin and Imran Ahmad Sajid, present a wealth of data to suggest that as far as Islamic Schools in Pakistan are concerned, they are not the factories for turning out suicide bombers the popular media like to portray. They present a well-argued case that underscores their point that deeper motivating factors are at work behind this vexing question. Islamic Fundamentalism is a factor in the mix of suicide terrorism but not the only or indeed the most important one. The history of the Indian sub-continent shows that religion is used in a national context to fight and

resist foreign occupation by powers that are perceived by the masses as unjust and oppressive militaries and their allies, and not to necessarily to bring about Sharia or Islamic rule in the land. Unfortunately, radical fundamentalists groups make use of such fears of foreign occupation to push their cause further towards extremist Islamic rule.

The third and final theme of this Special Issue deals with the use of cyber space for terrorism and radicalism purposes. The first article outlines the conceptual foundation for understanding the role social media can and does play in relation to spreading the threat and growth of terrorism, especially 'home-grown' terrorism. The utility of social media applications (eg. Facebook, Twitter, You Tube) to recruit, communicate and train terrorists is explored through the perspective of Knowledge-Managed Policing (KMP). The authors' review of the extant literature from military, academic and public open sources presents a disturbing picture of the multiple pathways Web 2.0 'social media' technologies provide for terrorists and militant extremists to utilise and develop cyber terrorism into a potent virtual battleground which police and security agencies must confront on a very uneven global playing field. Furthermore, they argue that the concept and practice of 'Knowledge-Managed Policing' (KMP) is highly relevant, timely and necessary perspective for policing/law enforcement/security agencies. Adopting a salient Knowledge Management approach can tip the competitive advantage towards policing the multitude of harms and threats that 'online terrorism' presents through the medium of the dark side of social media for Civil Society.

The last article in this Special Issue addresses the issue of cyber-crime in India and the Indian Government's response to the challenges it presents. Just as counter-terrorism policy in the EU has sought to harmonize laws to enhance effectiveness, this article documents what the Indian Government has done and is seeking to do to harmonize IT Laws to ensure cyber security. One of the more interesting initiatives by the Government to combat cyber-crime is the establishment of CERT-In, a well quipped organization of the Department of Information Technology, Ministry of Communications and Information Technology, within the Government of India. As the author points out CERT-In provides Incident Prevention and Response services as well as security quality management services and is designated to serve as the National agency to execute the various functions under the umbrella of cyber security.

Finally, I am especially delighted to have been asked to act as the Guest Editor of this Special Issue.

Dr. Geoff Dean
Associate Professor
Australia

Policing the Perilous Euroland: Countering Terrorism and Radicalization in Europe

Monica den Boer & Irina Wiegand

Abstract

Counter-terrorism is not a completely new arena of activity in the European Union. The Member States have cooperated since the early seventies, when terrorism was rife in various countries. The terrorist attacks of 9/11 have propelled the issue back onto the policy agenda, and joint efforts have been amplified by the attacks in Madrid (March 2004) and London (July 2005). Recently, concerns have been voiced over the resurgence of violent right-wing extremism. In contrast to the seventies, the EU can now encourage intensive cooperation between the jurisdictions of the Member States, as it is has established an Area of Freedom, Security and Justice. In this article, we discuss the three main planes of cooperation, namely the strategic, the regulatory and the agency level of cooperation. Finally, we analyze how nation states have responded to the call for European cooperation in the field of counter-terrorism.

Keywords

Terrorism, Radicalization, Europe, Strategy, Regulation, Law, Sovereignty, Europol, Eurojust SitCen

Introduction

The European Union (EU), which currently consists of 27 Member States, perceives terrorism and radicalization as a profound security threat, particularly after "9/11". The attacks which took place on 11 March 2004 in Madrid and on 7 July 2005 in London brought the security threat even closer home to the 500 million inhabitants in the EU. Terrorism had been on the agenda of the EU since the mid seventies, as several EU Member States had a long experience with terrorism (Schmid, 1983). Some Member States, like Spain and France, still face a considerable challenge from the Basque separatist movement ETA and from the Corsican independency movement. Despite the continuing attention for Islamist extremism, European countries have recently been alarmed by forms of violent right-wing extremism. Examples are the mass murder by the radical extremist Anders Breivik in Norway on 22 July 2011[1], and a string of racist murders by neo-Nazis in Germany[2] (Goodwin, 2011; Kaya, 2011).

Hence, despite the fact that the diagnosis of terrorism tended to shift to networked, Al Qaida inspired transnational terrorism, there is still a preoccupation with domestic groups that work on the basis of an entirely different ideology. The EU defines terrorism in terms of its constitutive elements and has imposed

legislation on the Member States which demands from the Member States that they criminalize acts of terrorism. Moreover, except for deep forms of legislative harmonization between the EU Member States, counter-terrorism as a policy field can also be characterized as a crowded policy arena with actors who represent different levels of governance (Den Boer and Monar, 2002; Peers, 2003). Within the EU, domestic and international agencies with a mandate in the field of counter-terrorism have become increasingly linked up, also because the EU has strongly encouraged a multi-dimensional approach to terrorism (Monar, 2007; Herschinger et al., 2010). A major concern is that agencies may fail to communicate or co-ordinate could hamper the prevention of a terrorist attack. Moreover, if agencies operate in a fragmented jurisdictional environment, terrorists may well be able to exploit legal loopholes.

Counter-terrorism in the EU goes along with a process of agencification. Bodies like the European Police Office *Europol* were given new tasks after the September 2001 attacks in the USA. Hence, it can be argued that the terrorist attacks of 2001, 2004 and 2005 provided a strong impulse to a comprehensive EU strategy against terrorism (Balzacq and Carrera, 2005).[3] The first response was to prompt a hyperactive regulatory agenda: the Extraordinary Council that took place after 9/11 launched 175 measures, among which several proposals for new legislation (Bures, 2006). The counter-terrorism instruments that have flown from this regulatory response include the EU Arrest Warrant, the EU Framework Decision on Terrorism, and a Framework Decision on Joint Investigation Teams, all of which are applied to a much wider range of criminal offences and all of which can actively be used by law enforcement.

Meanwhile, the policy issue of terrorism had matured into a more strategic, coherent and comprehensive programme. Even after 9/11 and the attacks that followed in Madrid and London, the EU Member States showed resistance in implementing the various EU-instruments that had been adopted by the Council. In the new decision-making régime of the Lisbon Treaty,[4] terrorism remains a sensitive area that rests firmly in the sovereign hands of the Member States. As a common field of policy-making, counter-terrorism has assumed a position between Justice and Home Affairs and Common Foreign, Defence and Security Policy. Meanwhile, the EU has drawn up a framework for the prevention, repression and prosecution of terrorism in Europe. The Lisbon Treaty, the Stockholm Programme[5] and the Internal Security Strategy[6] open up new avenues for counter-terrorism initiatives. Several other measures have since been adopted which can be regarded as a response to terrorism.

Below, we will discuss the EU effort against terrorism and radicalization in more detail. The first section of the article focuses on the strategic response of the EU, which has gradually evolved from a fragmented ad hoc response to a more integrated long term response which is based on selected policy priorities. Second, we will map the regulatory response of the EU and provide an overview of the main instruments that have been adopted by the EU in order to fight terrorism through law enforcement cooperation, information-sharing, crisis-management and the criminalization of acts of terrorism. Third, we will describe the way in which relevant agencies and counter-terrorism networks in the EU have been given various responsibilities in counter-terrorism. Fourth and finally, we devote a section to the way in which Member States have responded to the EU-strategies, policies and instruments.

The Strategic Response

When the terrorist attacks took place on 9/11, the EU immediately declared its solidarity with the United States. An extraordinary council was convened very soon after the events which amounted to a listing of policy ambitions to be realized. Despite the political endorsement of this activity, there was an absence of a real strategic perspective. With the attacks that took place in Madrid and London, and a series of other anxieties spurred on by single attacks which were motivated by extremist Islamist ideologies, the Member States of the EU realized it was time for real action and a more consistent strategic programme against terrorism. Despite the salience of terrorism as a security topic, this proved not to be an easy task. One obstacle was that the institutions of the EU – the European Commission, the European Parliament and the European Court of Justice – had marginal power in this field, as counter-terrorism is traditionally in the sovereign hands of the Member States. In the particular field of counter-terrorism, this boils down to a non-intervention principle, which means that the EU has no sanction powers, if a nation state in the EU refuses to comply with regulatory decisions. This contrasts to other fields in the EU, such as the Common Agricultural Policy.

A second obstacle flows from the situation that the responsible agencies in the Member States have engaged in longstanding forms of cooperation, but none of them had been fully institutionalized at EU-level. Counter-terrorism cooperation was mostly networked and - when it came to the exchange of operational intelligence - bilateral (Den Boer et al., 2008).

A third obstacle is that the experience with terrorism is (fortunately) infrequent (Dahl, 2010), but this implies that criminal justice systems and law enforcement bodies are not traditionally geared towards giving terrorism and radicalization top priority in their work. In fact, in most Member States law enforcement organizations

face restructuring exercises due to budget cuts and the drive for more efficiency, and they struggle with scarce capacity. A fourth reason is that counter-terrorism in the EU has been a policy which is situated at different levels of governance (Herschinger et al., 2010). It depends strongly on the political-administrative system of each EU Member State how, where and when efforts are invested in the fight against terrorism and radicalization. In some countries, counter-terrorism is high on the agenda and can be imposed top-down; in other countries, with a strongly decentralized character, such as The Netherlands and Germany, local and regional governance are important loci of power where the participation in the policy agenda is relatively high. Later in the article, we will return to domestic differences.

Despite these obstacles, the EU has gradually managed to steer its own course, even to the extent that one may now speak of a "European approach to terrorism". Important elements of the EU counter-terrorism strategy are prevention and multi-disciplinary cooperation. Since 2005, the EU has built its counter-terrorism strategy on four pillars, namely prevent, protect, pursue and respond.[8] The language of this strategy strongly resembles that of the British national response to terrorism. The main objectives of the EU strategy against terrorism are the cooperation with third countries (for instance with South East Asia), the respect for human rights, the prevention of recruitment into terrorism, the protection of potential targets, the investigation and prosecution of acts and suspects of terrorism, and the improvement of the capability to respond to and to manage the consequences of terrorism.[9]

The prevention pillar of the EU strategy aims at combating recruitment into terrorism and radicalization. It seeks to do so by identifying the instruments, methods and communication they use. It is acknowledged that this terrain of activity belongs to the EU Member States themselves, but the EU plays the role of coordinator and stimulator of the exchange of good practices and information. The protection pillar seeks to decrease the vulnerability of targets, and in this context, several initiatives have been taken in the context of border and transport security, as well as the protection of critical infrastructures. In the prosecution ("pursue") pillar of the EU counter-terrorism strategy, one seeks to bolster the judicial apparatus to disrupt terrorist organizations by making it more difficult to get access to weapons, explosives and finances. It is in this pillar that information exchange between the relevant EU agencies is strongly encouraged, assisted by the availability of several EU-wide databases and information-sharing agreements. As we will see in the next section, several legislative instruments have been adopted to fight money laundering and terrorist financing. The fourth pillar of the EU strategy revolves around response through media coordination, assistance to victims and help in civil military EU crisis management operations.

Progress is reviewed every six months by the Council, and each Presidency organizes a high-level political dialogue on terrorism. The counter-terrorism strategy is complemented by a detailed action plan which lists the relevant measures. The Committee of Permanent Representatives (who represent the Member States in the EU) monitor progress in detail on a regular basis, and it is provided that the Counter-Terrorism Coordinator and the European Commission perform regular follow-up and updates.

The Regulatory Response

The 9/11 events have led to a series of new legislative measures. The EU has taken a broad approach to counter the terrorist threat and introduced a "genuine EU counterterrorism policy" (Bures 2006: 60), internally, as well as externally.

On 27 December 2001, the first EC measure to fight terrorism in the aftermath of 9/11 was adopted. By regulating that funds, financial assets, and economic resources of those people and groups involved in terrorist activities and listed in the annex of the regulation are to be frozen, EC Regulation 2580(2001) provides for substantive measures to fight terrorism. In addition, banks and other financial institutions should provide information about those individuals and groups.[10] The list of names has been updated on a regular basis.

As Regulation 2580/2001 only covers terrorist groups not related to the Taliban, Osama bin Laden or Al Qaida, EC Regulation 881(2002), which was adopted in May 2002, established another list.[11] This list, which refers to individuals and entities related to the Taliban, Osama bin Laden or Al Qaida was set up by the UN and merely converted into EU law.[12]

The 2002 adopted 'Council Framework Decision on combating terrorism,' which includes a definition of the term terrorism, builds the cornerstone of the EU's fight against terrorism. It provides a definition of terrorism and terrorist groups and regulates the punishment of terrorist offences, which include inciting, aiding, or abetting terrorists and terrorist crimes. The definition establishes the core of the Framework Decision and basically incorporates the content of the by then twelve existing UN Conventions on terrorism. In 2008, the Framework Decision on combating terrorism was amended, with the Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.[13] These two Framework Decisions have led to a minimum harmonization in criminal matters related to terrorist offences.

In June 2002, the 'Framework Decision on the European arrest warrant and the surrender procedures between Member States' was adopted.[14] For 32 offences, the European Arrest Warrant makes the arrest and transfer of suspects possible without formal extradition procedures, by abolishing the principle of double criminality and

allowing for extradition of nationals of the surrendering state. A final measure that was adopted before the first large Islamist terrorist attack on European soil occurred is the 'Council Framework Decision on joint investigation teams' in June 2002.[15] It regulates that two or more Member States can set up joint investigation teams for a limited period of time - combating terrorism is the priority of these teams.

Immediately following the terrorist attacks in Madrid and London in March 2004 and July 2005 respectively, the EU adopted new counter-terrorism strategies. It was an important element in the Hague Programme, which was adopted in May 2005, and explicitly laid down in the new EU Counter-Terrorism Strategy, adopted in December 2005, serving as guidelines for the future, but not constituting new legal measures.[16]

The next legislative step was the amendment of the existing mechanism on information exchange of convictions in November 2005**.** To further facilitate cooperation in criminal matters, the Proposal for a Council Framework Decision on the European Evidence Warrant was adopted in July 2006, which enables Member States to obtain documents and data from one another for the use in criminal proceedings, thereby leading to faster procedures. The European Evidence Warrant was finally adopted in 2008.[17]

A number of different information systems have also been implemented, such as the Visa Information System in early 2008. Additionally, the Data Retention Directive was adopted and has meanwhile been implemented by almost all EU Member States. The Directive came into force on May 3, 2006, and aims at further harmonization between Member States.[18] It requires providers of electronic communications services and networks to retain traffic data related to emails and telephone calls for at least six months and up to two years from the date when a call was made, an email sent, or a website was visited. Information to identify the originator and recipient of the calls or emails is included, as well as the time, date, and length of the call or email. Internet telephony is also included along with calls to and from cell phones and landlines. In accordance with national law, these data have to be made accessible to the police for investigation purposes. It updates and in fact reverses the E-Privacy Directive, which was adopted in 2002, an in general did not allow for the storing of data.

Moreover, the “Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union” was adopted, which aims at faster exchange of information and data, for example by setting up time frames for responding to requests.[19]

As already mentioned, in 2007, an amendment of the Framework Decision on combating terrorism was proposed, which was adopted in 2008. By this amendment, the list of terrorist offences includes provocation to commit terrorism, as well as recruitment and training for terrorism. The UN called on its Member States to criminalize these acts in 2005.[20]

Hence, in the aftermath of 9/11, the EU has accelerated the legislative measures to counter the terrorist threat, by implementing UN measures on behalf of the Member States. Most counter-terrorism instruments were introduced immediately after 9/11. A second wave of new measures was triggered by the attacks on European soil in 2004 and 2005. Table 1 summarizes the main regulatory EU instruments in the field of counter-terrorism.

The Agency Response

Europol

The objective of the Europol,[21] which was established by virtue of the Maastricht Treaty that entered into force in 1992, is to improve the effectiveness and co-operation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other forms of international crime where two or more Member States are affected. Its mandate is to facilitate the exchange of information between the Member States. This means that Europol has no operational or executive mandate, but that it obtains, collates and analyses information and intelligence. Originally, Europol's investigations were to be limited to unlawful drug trafficking, trafficking in nuclear and radioactive substances, illegal immigrant smuggling, trade in human beings and motor vehicle crime. Subsequently, its mandate was gradually expanded by the EU Justice and Home Affairs Council.

Terrorism was added to Europol's mandate in 2000, only one year after the agency became operational.[22] At first, it was deemed politically undesirable to include anti-terrorism in the Europol-mandate, as there was a lack of a single definition of terrorism and as it would have implied the handling of very sensitive and proactive intelligence. However, the continuous struggle with terrorism in some Member States, notably Spain and the United Kingdom (UK), added significant pressure on the Justice and Home Affairs Council to include counter-terrorism in the mandate of Europol. Notwithstanding this political green light, Member States have remained reluctant to share intelligence and to give up their national sovereignty in law enforcement matters, which has made it difficult for an agency like Europol to prove its added value. The Council Decision on the exchange of information and co-operation concerning terrorist offences sought to improve upon this situation.[23] A

Council Decision changed the status of Europol into a communautarian agency, which *inter* alia, give the European Parliament more budgetary scrutiny powers[24] (De Moor and Vermeulen, 2010).

A leading role on terrorism by Europol was not claimed, partly because Europol was still not regarded as the agency with which national law enforcement agencies and security agencies wanted to share their intelligence, partly also because Europol was without a director between June 2004 and February 2005 (Keohane, 2005, p.20). Initially, Europol established a team of counter-terrorist specialists, with – in principle – two liaison officers from each EU Member State, one from the police and one from the intelligence service.[25] Europol was also requested to update the Directory of Specialised Counter-Terrorism Competences, Skills and Expertise[26] (Den Boer, 2003: 200).

While there was an ad hoc delivery of data to Europol in the field of terrorism, resulting from live ongoing investigations, in 2004 there was still 'no structured communication of (security) intelligence information' to the Analysis Work File 'Islamic Terrorism' at Europol which was assigned by the European Council on 21 September 2001 in setting up the Counter Terrorism Task Force (CTTF) at Europol (Hojberg, 2004: 52). In June 2004, the JHA Council decided to grant a supplementary budget to Europol to reinforce the operational intelligence analysis capacity, which meant that the intelligence analysis staff working at Europol could be more than doubled (Hojberg, 2004: 55). Europol also convened regular High level counter-terrorism experts meetings to discuss common problems related to terrorism and the responses of the agency to terrorism. In 2006, Europol supported around twenty "live" investigations in several Member States into Islamist terrorism (De Vries, 2006: 3).

The Counter Terrorism Task Force was requested to collaborate directly with American counterparts. The Director of Europol was instructed to conclude an 'informal agreement', pending a formal one, to be concluded on 16 November 2001.[27] The agreement would provide for 'the exchange of liaison officers between Europol and US agencies that are active in the policing sector. Moreover, the Director of Europol was requested to open negotiations with the USA on the conclusion of an agreement that included the transmission of personal data.[28]

After the terrorist attacks on 11 March 2004 in Madrid, the co-operation between Europol and the national security services was to be advanced, which led to the re-activation of the Counter Terrorism Task Force.[29] In the year 2005, Europol supported 20 ongoing terrorist investigations and two Analytical Work Files (AWF's) were in operation. Support was given to the anti-terrorism branch within Scotland Yard. Europol Liaison Officers (ELO) assisted the intelligence gathering after the event by working closely with the investigation team. Europol also

seconded a liaison officer to SitCen (see below) in order to avoid duplication of efforts. Europol seeks to assist Member States in identifying terrorist networks, to analyse interaction between international terrorism and organized crime, and to develop co-operation with relevant international organizations. This strategy can only be successful if the Member States share information and intelligence with Europol, and –after several legal instruments[30]- this is still seen as a major hurdle in the effectiveness of this agency. Relevant in this regard is that the European Commission wanted Europol to take a lead in advancing intelligence-led law enforcement by accommodating monthly meetings between the national criminal intelligence services of the Member States. Furthermore, there is the Council Decision on the transmission of information resulting from the activities of security and intelligence services with respect to terrorist offences intends to strengthen the relations between Europol and the national security and intelligence services by establishing national contact points in the Member States for the effective transmission of data.[31] Finally, Europol is in charge of producing the annual EU Terrorism Situation and Trend Report (TE-SAT).[32]

Eurojust

In order to improve judicial co-operation between the Member States and to overcome obstacles in mutual legal assistance procedures, Eurojust was established by virtue of the Tampere European Council on 15 and 16 October 1999. However, it was 9/11 that gave Eurojust a genuine boost. The decision to formally create Eurojust was adopted by the JHA Council of 6 and 7 December 2001. On 28 February 2002, the Council adopted the Decision setting up Eurojust.[33] (Den Boer 2003: 200ff). The mandate of Eurojust is to stimulate and improve the co-ordination of investigations and prosecutions between competent authorities in the Member States, for instance on mutual legal assistance or extradition. Eurojust is competent for the co-ordination of judicial investigations on the types of criminality for which also Europol is responsible. Following the Extraordinary Council on 21 September 2001, Eurojust had to pursue a strengthening of 'co-operation between anti-terrorism magistrates.' Like Europol, the agency was asked to intensify its co-operation with anti-terrorism magistrates in the USA. Eurojust is claimed to have been instrumental in avoiding the bombings at the Strasbourg Christmas market, the bombings in Belgium in Kleine-Brogel (a military base), and a bombing attack against the US Embassy in Paris (Nilsson, 2004: 19).

Eurojust organizes regular strategic meetings on terrorism, with representatives from all over the EU. It has created a Terrorism Team, which meets almost every week, and which aims at establishing a centre of expertise within Eurojust regarding terrorism, at ensuring that terrorism co-ordination meetings are well-structured and well-organised, at enhancing the exchange of terrorism-related

information between the nominated national experts on terrorism, at maintaining a general database of legal documents related to terrorism, at defining a better approach to the receipt and handling of terrorism information from open and closed sources, and at maintaining contacts with working parties and meetings in Brussels on topics related to terrorism. Following a former Council Decision,[34] the Eurojust Terrorism Correspondence team was called into being with national correspondents for terrorism matters with access to information from judicial authorities on persons, groups and entities suspected of terrorism and as listed in the EU Common Position 2001/931/CFSP. A later Council Decision 2005/671/JHA of 20 September 2005 repealed the former Council Decision, and was regarded as a qualitative and quantitative improvement in the exchanges of information, as it would considerably broaden the scope of information to be transmitted to Eurojust. The relevant Council Decision entered into force on 30 September 2005 and had to be implemented by the EU Member States by 30 June 2006. The number of terrorism-related cases dealt with by Eurojust was 28 in 2010, compared to 21 in 2009.[35] The highest percentage of criminal activities reported to Eurojust relate to drug trafficking and fraud.

SitCen

The EU Joint Situation Centre (SitCen) was created in 2002 and provides Member States with strategic analyses of the terrorist threat. It is based in the Council Secretariat and it reports to the EU High Representative and Secretary General of the European Council. SitCen is composed of about 45 (mostly seconded) national experts from intelligence and security agencies, including military ones! SitCen employees analyze intelligence assessments from the Member States based on national intelligence, open sources and diplomatic reports, and in turn provide Member States with threat assessments. National officials decide which information they send to SitCen. External assessments are combined with information from internal security agencies, and from Europol and the Counter Terrorism Group. SitCen produces reports from European politicians and ambassadors and these reports are essentially of a diplomatic or preventive nature, but not targeted at identifying or striking particular terrorists.

Anti-terrorism Co-ordinator

After the explosion of the railway bombs in Madrid on 11 March 2004, 175 measures were adopted in the form of a Roadmap, mainly because it was acknowledged that many of the originally intended counter-terrorism measures had not been adopted or implemented. A European Council Declaration on Combating Terrorism was concluded on 25 March 2004. One of the objectives included the development of mechanisms for the co-operation and promotion of effective systematic collaboration between police, security and intelligence services. It was decided that this multi-disciplinary co-operation between domestic services and

international services was subject to coordination by an EU anti-terrorism co-ordinator, who would be accountable to the Secretary General of the European Council or High Representative. The task of the EU anti-terrorism co-ordinator is to persuade the Member States to implement agreed EU anti-terrorism measures, but it should be reminded that the CT-coordinator does not have a budget or legislative powers, that he is not in the position to chair meetings and he does not attend relevant meetings at NATO (Keohane, 2005: 18). However, the EU anti-terrorism co-ordinator interacts directly with the national governments, which may hamper the potential of the Commission to co-ordinate anti-terrorism efforts across the different directorates with a competence in the field of counter-terrorism. Except for the CT-coordinator, the EU has a Council Working Group on Terrorism (coter) (Bergenstrand, 2004: 87), a Police Working Group on Terrorism (PWGOT), and the Counter Terrorism Group (Bergenstrand, 2004: 88; De Vries, 2006: 3; Wiebes, 2004: 119), and the Member States participate in the Club de Berne (Bergenstrand, 2004: 85; Keohane, 2005: 31).

Concluding Notes on National Implementation

In the ten years that followed 9/11, the EU has emerged as a security actor in its own right (Curtin, 2011). It has shown the capacity to respond to a security crisis through a political strategy, agencification and regulation. Despite the fact that counter-terrorism is deeply embedded in the national systems of the Member States of the EU, the joint efforts have amounted to coordinated cooperation and standardization of practices, for instance in the field of information exchange and the transfer of suspects. However, between the Member States there are still considerable differences. This is due to the fact that they have different experiences with terrorism, legal traditions and cultural perceptions of privacy.

Most instruments in the field of counter-terrorism have been adopted in an intergovernmental realm of decision-making. This means that instruments like the Framework Decisions on combating terrorism or on the European Arrest warrant, had to be converted into national law. The Member States have a certain leeway on how and when to implement the supranational instruments in their domestic laws. In addition, the competencies in the field of security mainly rest with the Member States, which also enacted a plethora of purely national laws in the field of counterterrorism. Therefore, despite all the developments on the EU level, "the European Union is still a long way from harmonization of counterterrorism policies of its Member States" (Van Dongen 2010, 237).

Differences are salient in three fields: the codification of criminal offences, criminal justice and procedure and the protection of data and privacy (Wiegand 2011). A quick scan through the implementation of the Framework Decision on combating terrorism in France, Germany, Italy, The Netherlands, Spain and the UK

exemplifies these differences in the fields of criminal offences and data and privacy protection when converting supranational EU law into domestic law. Especially in the latter field, the states have adopted numerous other laws, such as widening the use of CCTV, extending DNA databases or increasing co-operation between different national police agencies and intelligence services within the different states, but also across them. In the field of criminal justice and procedure, most newly adopted measures, such as extensions of police custody or allowance for interrogations without legal counsel, were taken on a purely national basis.

The 2002 Framework Decision on Combating Terrorism establishes a definition of the terrorism and lists a number of terrorist criminal offences, as well as the maximum possible sentences for these. It thereby aims at a minimum harmonization of the punishment of terrorist crimes. Prior to the implementation of the Framework Decision, the six relevant states all had different acts covered in their national law. The Netherlands did not have a special terrorist legislation prior to the implementation of the Framework Decision. The other five states all had terrorist crimes covered in their domestic legal systems, but each to a different extent. France, Spain and the UK already included all offences in their domestic legislation before the adoption of the Framework Decision, whereas in Germany and Italy, only domestic terrorism was a crime, but not international terrorism. Both countries added an international dimension of terrorism to their criminal codes immediately after 9/11. Italy further added conspiracy and support for conspiracy of terrorism, which was not covered in Italian law before.[36]

After the adoption of the Framework Decision on Combating Terrorism, Germany added 'terrorist intention' as an element of crime in 2003 and The Netherlands implemented the regulations of the Framework Decision in 2004, in order to comply with their obligation under EU law. By adding conspiracy to the law, The Netherlands went further than the EU required. France, but especially the UK added a number of additional criminal offences to their criminal codes not covered in supranational law, such as, in the UK, the possession of terrorist materials, even if not intended for the perpetration of a terrorist crime or the eliciting, publishing, or communicating of any information that could be useful for a terrorist attack.

The amendment of the Framework Decision in 2008 led to the adoption of further legislation. Especially in case of Germany and The Netherlands this is visible: both countries adopted laws with regard to preparation of terrorist crimes and participation in terrorist training camps in 2009. Italy had introduced these acts already in 2005, after the attacks in Madrid and London, whereas France, Spain and the UK had them covered prior to 9/11. Spain stands out in the comparison of these

six sates, as it did not introduce any new legislation with regard to terrorist crimes, with the exception of the widening of the concept of incitement in 2010 in order to comply with the amendment of the Framework Decision of 2008.

The Framework Decision on Combating Terrorism has led to a harmonization of national counter-terrorism laws. This effect can be observed in case of countries which had no or only limited legislation on counter-terrorism before, like the Netherlands or Italy and Germany. In this way, the Framework Decision led to an approximation of laws in the Netherlands, Italy, Germany and Spain, but as France and even more the UK has added a number of terrorist offences not covered by any supranational instrument, which the other states did not, the EU Member States area still characterized by a diversity of counter-terrorism legislation. Counter-terrorism cooperation between in the EU has become an irreversible process. With stronger EU institutions, we may witness a more profound process of strategic and legislative harmonization in the future.

Endnotes

[1]"The Norway attacks: Manifesto of a murderer", *The Economist*, 24 July 2011; http://www.economist.com/blogs/newsbook/2011/07/norway-attacks; accessed 20 December 2011.

[2]"Germany's Shocking Neo-Nazi Killers: How Did They go Undetected?", *Time World*, 17 November 2011; http://www.time.com/time/world/article/0,8599,2099616,00.html, accessed 20 December 2011.

[3]The Ministers of Justice and Internal Affairs convened on 13 July 2005 and endorsed the need for a collective strategy against the terrorist threat.

[4]Treaty of Lisbon, amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, Vol. 50, 17 December 2007.

[5]European Council, *The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens*, OJ C 115/1, 4.5.2010.

[6]Council of the European Union, *Draft Internal Security Strategy for the European Union, "Towards a European Security Model*, 23 February 2010, 5842/2/10, http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf

[7]As our article primarily seeks to offer an overview, we neither discuss issues such as governance, accountability, human rights, data protection or jurisdiction (see e.g. Hillebrand, 2010; Kaunert, 2010; Curtin 2011; Wolff *et al*., 2011), nor external relations and defence policy of the EU with regards to terrorism and radicalization (see e.g. Cremona et al., 2011).

[8]Council of the European Union, 30 November 2005: The European Union Counter-Terrorism Strategy. Available at: http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf; accessed 12 December 2011; see also Action Plan to Combat Terrorism, 13 February 2006 (http://register.consilium.europa.eu/pdf/en/06/st05/st05771-re01.en06.pdf; accessed 12 December 2011); Implementation of the strategy and action plan to combat terrorism of 19 May 2006 and of 12 December 2005 (http://register.consilium.europa.eu/pdf/en/06/st09/st09589.en06.pdf; http://register.consilium.europa.eu/pdf/en/05/st15/st15704.en05.pdf; accessed 12 December 2011).

[9]http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33275_en.htm; accessed 12 December 2012.

[10]Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism. Available at: http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&model=guicheti&numdoc=32001R2580; accessed 15 December 2011.

[11]Council Regulation 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al Qaida network, and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan. Available at http: //eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&model=guicheti&numdoc=32002R0881&lg=en ; accessed 15December 2011.

[12]The list was introduced by the UN with Resolution 1267(1999) and implemented in the EU in 2000 with Council Regulation EC 337(2000), which was updated with EC Regulation 881/2002.

[13]Council Framework Decision on combating terrorism. Available at: http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002F0475&model=guichett; accessed 15 December 2011 and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. Available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008F0919:EN:NOT; accessed 15 December 2011.

[14]Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002F0584:EN:NOT; accessed 15 December 2012.

[15]Council Framework Decision of 13 June 2002 on joint investigation teams. Available at: http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002F0465&model=guichett; accessed 15 December 2011.

[16]Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union. Available at: http: //eurlex.europa.eu/LexU riServ/LexUriServ.do?uri=CELEX:52005XG0812%2801%29:EN:NOT; accessed 15 December 2011.

[17]Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008F0978:EN:NOT; accessed December 15, 2011.

[18]Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Available at http: //eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT; accessed 15 December 2011.

[19]Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006F0960:EN:NOT ; accessed 15 December 2011.

[20]S/RES/1624/2005 Threats to International Peace and Security. Available at http: //daccessods.un.org/access.nsf/Get?Open&DS=S/RES/1624%20(2005)&Lang=E&Area=UNDOC; accessed 15 December 2011.

[21]Council Act of 26 July 1995 drawing up the Convention on the establishment of a European Police Office, Official Journal C316, 27.11.1995.

[22]Council Decision 99/C 26/06 [Official Journal C 26 of 30.01.1999], Council Decision of 3 December 1998 instructing Europol to deal with crimes committed or likely to be committed in the course of terrorist activities against life, limb, personal freedom or property.

[23]Council Doc. No. 2005/671/JHA, 20 September 2005.

[24]Council Decision of 6 April 2009 establishing the European Police Office (Europol), OJ L 121/37, 15.5.2009.

[25]bjective 31, doc. 12759/01.

[26]SN 3926/6/01 REV 6; Joint Action 96/610/JHA of 15 October 1996, adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on the creation and maintenance of a Directory of specialized counter-terrorist competences, skills and expertise in the Member States of the European Union, OJ L/273 of 25.10.1996.

[27]Draft Council Decision amending the Council Decision 2000/C 106/01 of 27 March 2000 authorizing the Director of Europol to enter into negotiations with 3rd States and non-EU related bodies. EUROPOL 85, Brussels, 16 November 2001.

[28]Objective 52, doc. 12759/01; Agreement between the United States of America and the European Police Office; https://www.europol.europa.eu/sites/default/files/flags/united_states_of_america.pdf (accessed 19 December 2011).

[29]European Council, "EU Plan of action on combating terrorism – Update', December 2004. http://eu.int/uedocs/cmsUpload/EUplan16090.pdf .

[30]E.g. Council Decision 2003/48/JHA of 19 December 2002, seeking to improve the exchange between Member States and EU bodies.

[31]Council Decision COM (2005) 695, 2005/0271 (CNS), not published in the Official Journal.
The 2011 report can be found at:
https://www.europol.europa.eu/sites/default/files/publications/te-sat2011.pdf (accessed 19 December 2011).

[32]Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63/1 (2002/187/JHA), 6 March 2002.

[33]Council Decision 2003/48/JHA of 19 December 2002 on the implementation of specific measures for police and judicial cooperation to combat terrorism in accordance with Article 4 of Common Position 2001/931/CFSP (OJ L 16, 22 January 2003).

[34]Annual Report Eurojust 2010, p. 33:
http://www.eurojust.europa.eu/press_releases/annual_reports/2010/Annual_Report_2010_EN.pdf; accessed 19 December 2011.

[35]Council Decision 2003/48/JHA of 19 December 2002 on the implementation of specific measures for police and judicial cooperation to combat terrorism in accordance with Article 4 of Common Position 2001/931/CFSP (OJ L 16, 22 January 2003).

[36] Annual Report Eurojust 2010, p. 33: http://www.eurojust.europa.eu/press_releases/annual_reports/2010/Annual_Report_2010_EN.pdf; accessed 19 December 2011.

References

Balzacq, T. and Carrera, S. (2005), *The EU's Fight Against International Terrorism. Security Problems, Insecure Solutions*. Brussels, Centre for European Policy Studies, CEPS Policy Brief No. 80, July 2005, available at http://www.libertysecurity.org/IMG/pdf/TheEU_sFightagainstInternationalTerrorism.pdf; accessed 8 December 2011.

Bergenstrand, K. (2004), 'The European Intelligence and Security Community and the Fight against Terrorism', in ICLN and EULEC, *European Co-operation against Terrorism*, Nijmegen: Wolf Publishers, pp. 83-89.

Bures, O. (2006), 'EU Counterterrorism Policy: a Paper Tiger?', in *Terrorism and Political Violence*, Vol. 18, Issue 1, pp. 57-78.

Cremona, M., Monar, J. and Poli, S. (eds.), *The External Dimension of the European Union's Area of Freedom, Security and Justice*, College of Europe Studies No. 13, Bruxelles: Peter Lang.

Curtin, Deirdre (2011), *Top Secret Europe.* Inaugural lecture, Amsterdam, University of Amsterdam.

Dahl, E. J. (2010), 'Missing the Wake-up Call: Why Intelligence Failures Rarely Inspire Improved Performance', in *Intelligence and National Security*, Vol. 25, No. 6, pp. 778-799.

De Moor, A. and Vermeulen, G. (2010), 'The Europol Council Decision: Transforming Europol into an Agency of the European Union', in *Common Market Law Review*, pp. 1089-1121.

De Vries, G. (2006), *The European Union and the fight against terrorism*, Presentation at the seminar of the Centre for European Reform, Brussels, 19 January.

Den Boer, M. (2003), 'The EU Counter-Terrorism Wave: Window of Opportunity or Profound Policy Transformation?', in Marianne van Leeuwen (ed), *Confronting Terrorism. European Experiences, Threat Perceptions and Policies*, The Hague: Kluwer Law International, pp. 185-206.

Den Boer, M., Hillebrand, C. and Noelke, A. (2008), 'Legitimacy Under Pressure: The European Web of Counter-Terrorism Networks', *Journal of Common Market Studies,* Vol. 46, No. 1, pp. 101-124.

Den Boer M. and Monar, J. (2002) 'Keynote Article: 11 September and the Challenge of Global Terrorism to the EU as Security Actor', *Journal of Common Market Studies*, Vol. 40, Issue supplement s. 1, pp. 11-28.

Herschinger, E., Jachtenfuchs, M. and Kraft-Kasack, C. (2010), 'International policing: embedding the state monopoly of force', in *Handbook on Multi-Level Governance*, Zürn, M., Wälti, S. and Enderlein, H. (eds.), Cheltenham: Edward Elgar, pp. 477-486.

Hillebrand, C. (2010), *The Democratic Legitimacy of EU Counter-Terrorism Policing: Challenges for Parliamentary and Judicial Scrutiny*, PhD, Department of International Politics, Aberystwyth University;

http://cadair.aber.ac.uk/dspace/handle/2160/4649?show=full (accessed 12 December 2011).

Hojberg, J. H. (2004), 'Building Trust and Developing More Efficient Sharing of Intelligence in Response to and Prevention of Terrorist Acts', in ICLN and EULEC, *European Co-operation against Terrorism*, Nijmegen: Wolf Publishers, pp. 49-57.

Kaunert, C. (2010), *European Internal Security. Towards supranational governance in the Area of Freedom, Security and Justice*. Manchester and New York: Manchester University Press.

Kaya, A. (2011), *Islamophobia as a Form of Governmentality: Unbearable Weightiness of the Politics of Fear*, Willy Brandt Series of Working Papers in International Migration and Ethnic Relations 1/11, Malmø, Malmø University (http://muep.mah.se/bitstream/handle/2043/12704/Willy%20Brandt%2011.1%20final.pdf?sequence=2; accessed 12 December 2011).

Keohane, D. (2005), *The EU and counter-terrorism*, London: Centre for European Reform.

Monar, J. (2007), 'The EU's Approach post-September 11: global terrorism as a multi-dimensional law enforcement challenge', in *Cambridge Review on International Affairs*, Vol. 20, Issue 2, pp. 267-283.

Nilsson, H. (2004), 'Judicial Co-operation in the European Union', in ICLN and EULEC, *European Co-operation against Terrorism*, Nijmegen: Wolf Publishers, pp. 15-36.

Peers, S. (2003), 'EU Responses to Terrorism'. *International and Comparative Law Quarterly*, 52, pp 227-243.

Schmid, A.P. (1983), *Political Terrorism – A Research Guide to Concepts, Theories, Data Bases and Literature*, Rutgers: The State University, Transaction Publishers.

Van Dongen, T. (2010), 'Mapping counterterrorism: a categorisation of policies and the promise of empirically based, systematic comparisons', in *Critical Studies on Terrorism*, Vol. 3, Issue 2, pp. 227-241.

Wiebes, C. (2004), 'De Problemen Rond de Internationale Intelligence Liaison', in *Justitiële Verkenningen: Inlichtingendiensten*, Vol. 30, No. 3, pp. 70-82.

Wiegand, I. (2011), *Towards Convergence? National Counter-Terrorism Measures in Western Europe: A Comparison of Counter-Terrorist Legislation in France, Germany, Italy, the Netherlands, Spain, and the UK after 9/11*. Unpublished PhD Manuscript, Bremen International Graduate School of Social Sciences.

Wolff, S., Goudappel, F.A.N.J., De Zwaan, J.W. (2011) (eds)., *Freedom, Security and Justice after Lisbon and Stockholm*, The Hague, T.M.C. Asser Press.

The author Monica den Boer teaches at the Police Academy of The Netherlands. Additionally, she is visiting professor at the College of Europe in Bruges and acting Member of the Committee on European Integration of the Dutch Advisory Council on International Affairs. Until recently she was a professor at the VU University Amsterdam. She obtained a PhD in 1990 from the European University Institute in Florence, and successively worked at Edinburgh University, the Netherlands Study Centre for Crime and Law Enforcement, the European Institute of Public Administration, Tilburg University, and the European Institute of Law Enforcement Co-operation. She was a member of the Dutch Iraq Investigation Committee, as well as the Defence Future Survey Group. Her research focuses on European internal security co-operation. She has published between 150 and 200 articles, chapters, working papers and books. Recent publications include "Ethics and Security" (ed., with Emile Kolthoff) and the Handbook on Good Policing (with Changwon Pyo) for the Asia-Europe Foundation ASEF. She can be reached at M.G.W.den.Boer@vu.nl

and author Irina Wiegand works at the University of Bremen and Jacobs University Bremen. After her studies in Political Science, Roman Languages and International Relations, she was a PhD Fellow at the Bremen International Graduate School of Social Sciences (BIGSSS). Her current research focuses on European approaches to terrorism, civil liberties protection in the fight against terrorism and domestic differences in countering the terrorist threat among EU Member States and she can be reached at iwiegand@bigsss.uni-bremen.de

Social Network Analysis of Terrorist Networks: Can it Add Value?

Mark Lauchs, Robyn Keast & Vy Le

Abstract

The study of terrorism includes the study of terror networks. The key method of studying networks is Social Network Analysis (SNA). This article aims to determine whether SNA can add value to the study of terror networks. We examine the existing research into terror networks including those that use SNA to reveal the nature of those networks. One of the most constructive approaches is the study of resilience of terrorist groups. We conclude that the use of SNA to study resilience will make the best contribution to ongoing research into terrorist networks and provides a good focus for both theory and practice of counter-terrorism.

Keywords

Terrorism, Terror Networks, Social Network Analysis, Resilience

Introduction

What is the value of social network analysis (SNA) to the study of terrorism? The study of terrorism has increased since the attacks of September 11, 2001. This time period has coincided with the increase in personal computer processing power allowing desktop operation of network analysis programs enabling academic researchers to use SNA mechanisms to study social networks. This is still a relatively young field of study, particularly in the terrorist arena. Nonetheless, the authors suggest that it will add a valuable realm of data to help understand how terrorist groups operate and can be combated.

Terrorism occurs through highly visible acts. Yet the operation of the terror networks is largely invisible, hidden within an opaque and loose structure of individuals and groups. This invisibility shields the internal operation and functioning of the networks from scrutiny and limits understandings of how to either engage with members to negotiate mutual outcomes, or disrupt, dismantle or destroy these entities. This article is not about the detailed intelligence work conducted by intelligence agencies. Rather it asks the question of what academics can learn about the nature of terrorist networks through SNA techniques.

The Nature of Terrorist Groups

Human society operates in networks of work, private relationships and broader social interaction. Most of these networks are mundane and open to the world. However, there are a category of networks that are hidden from view. These *dark*

networks are those where the network achievements come at the cost of other individuals, groups or societies and, in addition, their activities are both 'covert and illegal' (Raab and Milward, 2003). Terrorist groups fall within this category.

A distinction must be drawn at this point between the two types of dark networks. An organised crime network wants to remain invisible to all but their customers. They operate without the scrutiny of law enforcement. Terror networks, on the other hand, must have some level of visibility to achieve their goals. A terror group uses terror (fear and violence) attacks to draw attention to their political goal. These attacks are necessarily public and the group must claim responsibility to draw the nexus between the attack and their campaign. Even as acts of extortion (meet our demands or we will attack again), a terror group must identify their existence and their goal as a necessary part of the extortion technique. This does not mean that the group is entirely visible. It must keep its membership, location, organisation and finances outside the public gaze. Nonetheless sufficient study has taken place on terrorist groups to distinguish their unique characteristics which can inform SNA study.

Terrorist networks, from SinnFein to Al Quaeda, have proven to be resilient entities; resisting persistent and focused attempts to dismantle. Gupta (2008) has identified three potential areas of vulnerability related to their membership. First, terrorist groups rely upon charismatic leaders to succeed (Gupta, 2008) . However, leaders can also be a point of vulnerability. Politically, "Through their vision these innovators 'connect the dots' for their followers, which not only suddenly allow them to see who they are in terms of a larger entity, but also a way out of their current predicament." People have a proclivity to follow leaders but the leaders need the skills to motivate to become successful leaders. Gupta states that leaders do this by creating a group identity: framing issues in a manner that accentuates this identity through anxiety based on difference. Through this process other groups are scapegoated with the blame for all the perceived wrongs suffered by the group members and an ideal is promulgated that will right these wrongs (Gupta, 2008). Without a strong organizational structure and engrained operating framework, leaders and other core roles within networks, such as commanders (those that direct operations) and brokers (those that connect the groups with cells and supporters), are essential elements directing the work of the networks. Without these roles the terrorist network lacks the institutional capacity to survive. However, within networks leadership is dispersed, with multiple people taking on various leadership roles. This makes the location of key leaders and other central roles difficult.

Second, terror groups are supported by a particular nature of membership. There are three types of member motivations:

- *Mercenaries* (greed) are those who participate solely for personal gain.
- *Ideologues* (ideology) are those who participate primarily out of desire to help the group.
- *Captive participants* (fear) are those who participate because the cost of not participating is too high. (Gupta, 2008)

If there is no money then the mercenaries will leave. If there is no leader then the ideological base of the group may dissipate. Finally, if the mercenaries and ideologues are gone then the captive participants will be free to cease involvement in the terror network. Thus, the identification and location of funding streams and funding connectors has the potential to starve the network of the resources needed to sustain a mercenary workforce.

Third, public support is essential as a source of volunteers, money, safe houses and protection against infiltration by the government. A network gets stronger when its base grows. When a group gets large enough it can recruit captive participants. When it loses its legitimacy and core memberships it gets depleted (Gupta, 2008). Thus groups survive through tapping into existing networks such as religious groups and unions and financing, through crime, other governments and tithes from supporters (Gupta, 2008). Conversely, terror groups die off when either: their political goals become irrelevant; through loss of leadership by embarrassment through military defeat, the leader being killed or imprisoned, or if the leader changes sides; or, the group achieves its goals (Gupta, 2008). Assuming anti-terrorist organizations do not want the latter, and that they are not in a position to change broader politics, then they need to pursue a policy of cutting off the terrorist group from their base, their finance or their leader. Each of these three potential areas of vulnerability can be better facilitated and enacted by studying the network of a terrorist group.

Social Network Analysis (SNA)

Network analysis is an empirical tool which can be used to identify, measure, visualize and analyze the ties between people, groups and organizations (Scott, 1991). It plots relationships between individuals or entities by representing them as nodes and showing their relationships by linking nodes with lines. Lines can have different depictions to indicate characteristics of links including frequency and method of contact. The nodes and lines form a network map that reveals relationships between members of the network such as gate keeping (controlling the network), liaisons and core and periphery members' (Sparrow, 1991). In so doing, it

uncovers the often hidden or opaque patterns of interaction and enables the underlying structure of relationships to become more apparent (Cross et al., 2002) . The graphical or mapping visualization capacity affords administrators and others charged with the responsibility for 'responding to terrorism' to more clearly and empirically examine the network topography, diagnose weak points and propose areas for intervention.

In addition to its visual contribution, the mathematical underpinnings of network analysis also generate network metrics that make it possible to gain deeper insights into the actual texture and operation of the networks. Social network analysis can be used to examine a network's resilience by analyzing vulnerability through identifying central nodes, the availability of alternate nodes to take the place of lost central nodes, and less-central but bridging nodes tying together remote sections of the network (Keast and Brown, 2005). Measures such as density (the level of connectivity) and centrality (the level of concentration) also provide important insights into the structural properties of dark networks.

Density is a measure of the number of actual connections compared to the total number of possible connections. Centrality measures how concentrated a network is; high concentration indicates that a small number of people control the flow of resources. Average Path Distance is an indication of how quick it is to navigate around the network. This measure provides insights into how close or removed certain actors are and, as a consequence, their level of knowledge. Closeness is a measure of the proximity that an actor has to all other actors in the network, and is related to the flow of information within a network. Betweenness determines the shortest path distance between every pair of actors in a network, and then measures the degree to which an actor appears on those paths. Actors that control information within a network will have much higher betweenness values than those who appear on the fringes.

The study of the social network basis of covert networks precedes the modern visualization revolution by decades. Erickson (1981) noted that covert networks must be studied using these techniques. Similarly Baker and Faulkner (1993) examined the nature of white collar crime networks and drew conclusions about the nature of how such a network must operate. A RAND study by Arquilla and Ronfeldt (2001) , *Networks and Netwars: The Future of Terror, Crime, and Militancy*, placed more emphasis on the organizational rather than social nature of the network.

SNA has already had extensive use in the analysis of organized crime groups. Since the 1930s, research into criminal interaction identified the significance of network structures in facilitating criminal activity (Sutherland, 1937). From the 1970s, studies into Italian-American and Sicilian organised crime families suggested that these groups were based upon social or familial networks, kinship

ties and shared cultural values within a community (Albini, 1971). The use of SNA as a method to analyse organised crime groups is well-motivated given that numerous scholars have argued that organised crime is, at a fundamental level, a product of overlapping and interrelated social relationships (Heber, 2009, Kleemans and de Poot, 2008, Bruinsma and Bernasco, 2004, McIllwain, 1999, Block, 1994).

Networks are seen as a more suitable structure for organised crime because they facilitate the flow of information, can adapt to changes in law enforcement responses and have the flexibility to deal with the associated risks inherent in all organised crime activities. Within an organised crime network, SNA techniques can identify network members that control information and how the removal of one or more members can inhibit the flow of information or alter the network's ability to adapt or perform at its best (Carley et al., 2002). This type of analysis is essential in destabilizing networks (Carley et al., 2002). Thus, the utility of SNA as an analytical framework is apparent given evidence that the structure of organised crime groups are shifting towards more flexible networks (von Lampe, 2009) and that the nature of information provided by SNA can potentially disrupt organised crime activity.

SNA and Terror Networks

One of the most important developments in the SNA field in the last decade has been the development of reliable visualization software packages that can be used on a desktop or laptop computer. The processing power of computers has made sophisticated data analysis a routine activity that can be performed with basic instruction in the packages software. It is no longer necessary for a researcher to have mastered the mathematics of SNA metrics. Most software packages like Analyst Notebook include the ability to produce SNA analytics literally with the 'click of a button'. It can, therefore, be expected that there will be a proportional growth in the use of these abilities as the price and power of SNA software increases. Visualization of a network provides a unique ability to study a network. Yang et al (2006) note that visualization of terror networks can reveal the subgroups within the network, the key players and how the members interact. Xu and Chen (2005) also noted the significance of visualization and using SNA. However, neither of these studies uses the full potential of SNA metrics to study the nature of the groups and draw testable hypotheses for the study of terrorist networks generally.

The published studies of terrorist groups are far less extensive than those of organized crime. This may be a result of the relative inaccessibility of data. However, the publicity attached to terrorism is much greater than that for organized crime and this has allowed some researchers to construct their own datasets of terror networks. This occurs in two ways. First, detailed media coverage of terror group activities can be sufficient to build a network map. For example, Krebs (2002) was able to map the 9/11 terror network through media reports in the New York Times,

the Wall Street Journal, the Washington Post and the Los Angeles Times. There are also increasingly detailed studies from independent research agencies such as RAND and especially the International Crisis Group, which can provide both intricate detail and high levels of reliability,

The arrival of accessible SNA software packages has led to a number of articles being published analyzing terrorist networks. Koschade (2006) studied Jemaah Islamiyah using SNA techniques to make significant findings about the strengths and weaknesses of the group. Mullins and Dolnik (2009) studied other Islamic terrorist groups. Memon et al (2008) found small world characteristics in terror networks. Many more studies are necessary before any reliable empirically based theories of terror networking can be developed.

Resilience of Networks

One of the most valuable contributions that academic study of terror networks can provide is an understanding of what makes a terror network resilient. The study of resilience is valuable in determining how to destabilize or break up a network. Reducing resilience increases vulnerability (Ayling, 2009). Studies of resilience should do more than just describe vulnerabilities such as central nodes or personalities. The removal of key personnel, such as the most central node, will not necessarily collapse the network (Milward and Raab, 2006). Resilient networks are flexible and adapt to survive. The adaption may take many forms from replacement of lost individuals through to a major reorganization of the network. The points of resilience are the characteristics that allow the network to avoid or recover from an attack. Thus we should be wary on conclusions about network vulnerability that assume the relationships within the network are static and do not account for adaptation. This does not mean that we should not attack a network by undermining its strength, but rather that we should avoid naïve assumptions as to what constitutes strength.

Long lasting networks are the most dangerous. Not only will they produce the largest quantity of attacks over their extended life, but they will have the longest time to learn from their mistakes, become terror veterans, and could be expected to produce the most effective attacks. Resilience is the capacity to survive environmental change and direct attack. Bakker et al (2011) proposed that resilience is 'dynamic' and networks should not be considered as fixed entities. When studying resilience researchers should also consider the nature of the external forces at work, the ability of a network to withstand these pressures (robustness), the ability to bounce back from attack (rebound) and their vulnerability to attacks by an 'informed actor', that is someone who knows the network.

Most of the SNA work on resilience has been conducted on organized crime groups. In the case of such a group it refers to the ability of that group to continue its

operations through a changing market and the direct interference of both competitors and policing agencies. Bouchard used environmental studies of resilience to develop a list of characteristics which are useful in determining network resilience: *vulnerability* referred to the likelihood of damage from a specific type of attack; *elasticity* is the system's ability to return to its original state after taking damage; and the network's *adaptive capacity* is its ability to change to reduce its vulnerability (Bouchard, 2007). The most common adaption by dark networks is to reduce their visibility either through reduced size or looser structures. (Bouchard, 2007). Dark networks suffer unique vulnerabilities, namely, visibility attracts unwanted attention, especially from law enforcement. Visibility may not be a weakness in itself but it increases that likelihood of investigation. Visibility can occur in two ways: a large, formal network will be more visible to outsiders than a small, loose network; and, a central node (a person with many connections in the network) will be more visible than a node with less centrality because he will be associated with a greater range of activity. Not all networks have a centre of gravity, or *core*, which retains authority over the *periphery* of the network and directs its operations. (Klerks, 2001, Morselli et al., 2007).

Milward and Raab (2006) point out that a dark network must follow certain steps to establish the network. First, they must find enough people for the network; a task usually met by finding members in the same proximal group. Erickson (1981) concluded that risk can only be controlled by relying on trusted members and through the use of a strict hierarchical operational structure. Milward and Raab (2006) identified three alternative criteria of resilience. First the members needed to have character traits that supported the network. Second, the members had to be able to trust each other. Third the network is more resilient if it has *connectivity robustness*, the ability to respond and recover from losses of critical nodes.

We have already noted that hierarchies are avoided to offset the risks of visibility. However, trust sets the boundaries of dark networks. A dark network must limit its membership to those it can trust, i.e. it must be a *closed network*, made up of people with strong relationships (Burt, 2005). Members of the closed network share information about the reputation of other members. A member's reputation is determined by expectations of the person's future performance based on his or her past performance within the group; repeated good performance builds an expectation of future good performance. According to Burt, "You trust someone when you commit to a relationship before you know how the other person will behave"(Burt, 2005). A good reputation is built by emulating behavior that reflects the group's norms; norms which are built up over the social history of the group. Thus a terrorist group's members have a reputation that rates their commitment to the ideology and their trust worthiness to both maintain secrecy and reliably fulfill

tasks. If a member of the group does not know a potential working partner they can obtain a reliable assessment of the person by seeking opinions other trusted group members.(Burt, 2005)

Krebs (2002) mapped the terror cell responsible for the 9/11 attacks. He reached some conclusions about covert networks. Once in a conspiratorial network like a terror cell, the members rely on strong ties. They cannot afford to make new acquaintances outside the network. Krebs said that the terrorists formed strong ties in the past, for example, through school, and had such ties with all the members of the group. They do not expose these ties lest they reveal their network. The ties also allowed for redundancy; though he does not explain how. Krebs also says the same ties made the network strong and resilient, but once again did not explain how.

Williams presented two mechanisms by which networks protect themselves (William, 2001). Some networks defend themselves by developing buffer nodes at the periphery to protect the core from police investigation. The peripheral members undertake the high profile activity while the core members would keep such activity at arm's length to ensure deniability of any criminal action and to reduce their visibility to observers outside the network (Williams, 2001). Second, a network could be compartmentalized so that the loss of one compartment would not bring down the entire network (Lauchs et al., 2011b, Lauchs et al., 2011a). Both the structures can be revealed through visualization and SNA. But there are nuances that must be recognized, for example, having a network core does not mean that this is the locality of the network leadership. Carley, Lee and Krackhardt (2002) demonstrate that the leaders may not have the most contacts in the network; a leader may only communicate with one lieutenant who then interacts with agents and allies. In such a group the leader is protected by the more central decoy should law enforcement make assumptions about targeting group members based on centrality. Removal of a central node or a broker would still inhibit the network's operation. Removing one node may not destroy the network if that node can be replaced by a new *emergent leader* to embody the leadership role or fill the network space (Carley et al., 2002). SNA can locate the true points of vulnerability in the network rather than simply the apparent leadership. It can also provide a clear picture of how information flows in the network.

Carley, Lee and Krackhardt (Carley et al., 2002) note that network destabilization can occur through a reduction in the rate of information flow in the network, a failure/destruction or significant slowing down of the decision making process, or a reduction in operational effectiveness – the ability to conduct its tasks. Latora and Marchiori (2004) point out that network efficiency measures how well communication flows in the network. They propose measuring the network efficiency of a group and attacking the nodes whose removal will bring about the

greatest reduction in efficiency, noting that, the best node to attack is not always that which has the most connections. Once again, these flaws can be mapped in the visualization software and analysed via SNA metrics.

Conclusion

The increase in personal computer power has made it possible for academics to map and analyse complex networks such as terrorist groups. Due to the recent advent of this area of study there have been few published studies of terror networks using SNA and visualization. SNA offers an extremely useful tool for understanding how terror groups form and operate. In particular, it allows the 'hidden' or opaque structure and relations of the networks to become more visible and, therefore, open to intervention. We suggest that the most important area to study is resilience of the groups, as long lasting groups are the most dangerous to the community.

SNA helps attack the resilience of groups by identifying membership links, money movements and information flows within a network. The metrics analyse the strengths and weaknesses of a network and allow targeting of the individuals whose removal will most effectively disrupt the terror group's operations. While academics are unlikely to be studying real-time information in the same manner as intelligence agencies, they can still develop theories about terrorist group structures and operations which will help everyone better understand the groups vulnerabilities and longevity.

References

ALBINI, J. 1971. *The American Mafia: Genesis of a Legend,* New York, Appleton-Century-Crofts.

ALBINI, J. 1971. *The American Mafia: Genesis of a Legend,* New York, Appleton-Century-Crofts.

ARQUILLA, J. & RONFELDT, D. 2001. *Networks and Netwars: The Future of Terror, Crime, and Militancy,* Santa Monica, RAND.

AYLING, J. 2009. Criminal organizations and resilience. *International Journal of Law, Crime and Justice,* 37**,** 182-196.

BAKER, W. E. & FAULKNER, R. R. 1993. The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry. *American Sociological Review,* 58**,** 29.

BAKKER, R. M., RAAB, J. & MILWARD, H. B. 2011. A preliminary theory of dark network resilience. *Journal of Policy Analysis and Management***,** n/a-n/a.

BLOCK, A. 1994. *East Side-West Side: Organizing crime in New York City 1930-1950,* New Jersey, Transaction.

BOUCHARD, M. 2007. On the Resilience of Illegal Drug Markets. *Global Crime,* 8**,** 20.

BRUINSMA, G. & BERNASCO, W. 2004. Criminal groups and transnational illegal markets. *Crime, Law and Social Change,* 41**,** 79-94.

BURT, R. 2005. *Brokerage and Closure: An Introduction to Social Capital,* New York, Oxford University Press.

CARLEY, K. M., LEE, J.-S. & KRACKHARDT, D. 2002. Destabilizing Networks. *Connections,* 24**,** 14.

CROSS, R., BORGATTI, S. & PARKER, A. 2002. Making Invisible Work Visible: Using Social Network Analysis to Support Strategic Collaboration. *California Management Review,* 44**,** 12.

ERICKSON, B. 1981. Secret Societies and Social Structure. *Social Forces,* 60**,** 22.

GUPTA, D. 2008. *Understanding Terrorism and Political Violence: The life cycle of birth, growth, transformation, and demise,* London, Routledge.

HEBER, A. 2009. The networks of drug offenders. *Trends in Organized Crime,* 12**,** 1-20.

IANNI, F. 1972. *A Family Business: Kinship and Social Control in Organized Crime,* New York, Russell Sage Foundation.

KEAST, R. & BROWN, K. 2005. The Network Approach to Evaluation: Uncovering Patterns, Possibilities and Pitfalls. *Australasian Evaluation Society International Conference.* South Bank, Brisbane.

KLEEMANS, E. R. & DE POOT, C. J. 2008. Criminal Careers in Organized Crime and Social Opportunity Structure. *European Journal of Criminology,* 5**,** 69-98.

KLERKS, P. 2001. The Network Paradigm Applied to Criminal Organisations: Theoretical nitpicking or a relevant doctrine for investigations? Recent developments in the Netherlands. *Connections,* 24**,** 13.

KOSCHADE, S. 2006. A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence. *Studies in Conflict & Terrorism,* 29**,** 559 - 575.

KREBS, V. 2002. Uncloaking Terrorist Networks. *First Monday,* 7.

LATORA, V. & MARCHIORI, M. 2004. How the science of complex networks can help developing strategies against terrorism. *Chaos, Solitons & Fractals,* 20**,** 69-75.

LAUCHS, M., KEAST, R. & CHAMBERLAIN, D. 2011a. Resilience of a corrupt police network: the first and second jokes in Queensland. *Crime, Law and Social Change***,** 1-13.

LAUCHS, M., KEAST, R. & YOUSEPFOUR, N. 2011b. Corrupt Police Networks: Uncovering hidden relationship patterns, functions and roles. *Policing and Society,* 21**,** 18.

MCILLWAIN, J. S. 1999. Organized crime: A social network approach. *Crime, Law and Social Change,* 32**,** 301-323.

MEMON, N., HICKS, D. L., HARKIOLAKIS, N. & RAJPUT, A. Q. K. 2008. Small World Terrorist Networks: A Preliminary Investigation

Applications and Innovations in Intelligent Systems XV. *In:* ELLIS, R., ALLEN, T. & PETRIDIS, M. (eds.). Springer London.

MILWARD, H. B. & RAAB, J. 2006. Dark Networks as Organizational Problems: Elements of a Theory. *International Public Management Journal,* 9**,** 333 - 360.

MORSELLI, C., GIGUÈRE, C. & PETIT, K. 2007. The efficiency/security trade-off in criminal networks. *Social Networks,* 29**,** 143-153.

MULLINS, S. & DOLNIK, A. 2009. An exploratory, dynamic application of Social Network Analysis for modelling the development of Islamist terror-cells in the West. *Behavioral Sciences of Terrorism and Political Aggression,* 2**,** 3-29.

RAAB, J. & MILWARD, H. B. 2003. Dark Networks as Problems. *J Public Adm Res Theory,* 13**,** 413-439.

SCOTT, J. 1991. Social Network Analysis: A Handbook. London: Sage.

SPARROW, M. K. 1991. Network vulnerabilities and strategic intelligence in law enforcement. *International Journal of Intelligence and CounterIntelligence,* 5**,** 255 - 274.

SUTHERLAND, E. 1937. *The Professional Thief by a Professional Thief,* Chicago, University of Chicago Press.

VON LAMPE, K. 2009. Human capital and social capital in criminal networks: introduction to the special issue on the 7th Blankensee Colloquium. *Trends in Organized Crime,* 12**,** 8.

WILLIAMS, P. 2001 Transnational Criminal Networks. *In:* ARQUILLA, J. & RONFELDT, D. (eds.) *Networks and Netwars.* Santa Monica: Rand.

XU, J. & CHEN, H. 2005. Criminal Network Analysis and Visualization. *Communications of the ACM,* 48**,** 8.

The author Dr. Mark Lauchs is a Senior Lecturer in the School of Justice, Queensland University of Technology in Australia. He is a former bureaucrat who now teaches and researches in the field of dark networks and corruption.

The author Assoc Prof Robyn Keast is from the School of Management, Queensland University of Technology in Australia. She is a former bureaucrat who researches and publishes extensively in the field of social network analysis.

The author Vy Le is a PhD candidate in the Faculty of Law, Queensland University of Technology, Australia. She is researching South East Asian drug networks operating in Australia.

Assessing Terrorist Risks: Developing an Algorithm - Based Model for Law Enforcement

Frederic Lemieux, James L. Regens

Abstract

Assessing the risk posed by terrorist groups has always been a challenge for national security intelligence analysts. The most noticeable obstacles are, on one side, the limited availability of reliable information about violent groups and, on the other side, the absence of objective as well as rigorous assessment methods. This paper aim to outline the basic principles of a risk-based approach to terrorism threat assessment, which integrates algorithm models in order to provide more accurate situational awareness and orient strategic decision-making process. This paper is divided in three sections: first we introduce the readers to the objectives of strategic terrorism risk assessment. Second, we provide a comprehensive critic of existing terrorism threat assessment. Third, we develop an alternative logic model based on several factors related to the threat, vulnerability and uncertainty (error term). Finally, the paper suggest a methodology that takes in account the integration of risk factors drawn from theoretical and "real life" law enforcement perspectives.

Keywords

Terrorism, Risk Assessment, Law Enforcement, Strategic Analysis

Introduction

The U.S. Department of Homeland Security (DHS) has implemented numerous anti-terror countermeasures in response to perceived threats over the past decade, and efforts are underway to develop others. Unlike natural or accidental man-made disasters, terrorists are adaptive and may shift their tactics, techniques and procedures (e.g., attack strategy) when countermeasures are employed. Moreover, when confronting adaptive adversaries, defenders also often have to operate under resource constraints including limited information for modeling terrorism risk. For example, understanding and assessing adversarial behaviors requires insights into motivations, intentions, and capabilities, but garnering those insights is difficult because we rarely can collect information directly from terrorists. As a result, assessing the risk posed by domestic and international terrorist groups and 'lone wolf' actors operating outside the context of formal groups is a daunting challenge for law enforcement intelligence analysts. Currently referred to as the "intelligent adversary" problem, the ability to estimate reasonable and defensible occurrences (or at least relative probabilities) for terrorism events is an important focus for research.

There are two critical obstacles that must be overcome to derive credible estimates to guide homeland security and law enforcement agencies: (1) the limited availability of reliable information about threatening groups or individuals; and (2) the need for rigorous objective and practical assessment methods. This paper proposes to surmount these barriers by identifying key metrics to design an algorithm-based model that facilitates integrating risk-based terrorism threat assessment into situational awareness and strategic decision-making for counter-terrorism (CT) strategies at the law enforcement level. The paper focuses on combining rigorous scientific research with law enforcement experience to design and calibrate the algorithm-based model. The proposed model can enhance intelligence sharing from the tactical/operational level to the strategic level by generating a common operating picture (COP) of the threat environment. Finally, a risk-based assessment using robust algorithm model can accelerate and validate decision-making to identify, assess, and implement CT strategic priorities by law enforcement agencies.

The long-term goal of this model is to develop effective intelligence-driven CT strategies that can help law enforcement to prevent attacks though identification of key variables related to engagement in terrorist activities, thereby enhancing the capability of analysts to 'connect the dots'. This application's objective is to assess the utility of algorithm-based models by integrating risk-based terrorism threat assessment into situational awareness and strategic CT decision-making by drawing on parameters outlined by law enforcement. Our central assumption is that a mathematical model that incorporates key variables identified through a combination of expert judgment grounded in field experience and empirical data can aid intelligence analysts in assessing the risk, prevalence, and trends of terrorist activity.

The relevance of this paper is rooted in the importance of analytical frameworks to generate strategic intelligence. Because formal or informal threat assessment techniques frame judgments about risk, the 'lenses' that analysts employ play decisive roles in developing actionable intelligence, making them the key to identification and disruption of terrorist planning (George and Bruce, 2008; Heuer, 1999). This underscores the inherent centrality of the analytical tools with which indicators and warnings are identified, interpreted, and placed into context.

Background

Ten years after the tragic attacks of September 11, 2001, the United States still remains at risk of being targeted by political violence at home and abroad. The past decade has revealed important lessons learned about deterring and/or preventing our adversaries from initiating successful terrorist actions. Retrospective analyses

underscore the effectiveness of the US intelligence community's CT activities as critical components in achieving success thus far. Since 9 / 11, most of those CT efforts have been focused on thwarting al-Qa'ida's (AQ) strategic reach at the international level; diminishing its operational capacity at the regional level (i.e., Afghanistan, Iraq, the Maghreb, Somalia, Yemen); preventing successful attacks at the domestic level; and, ultimately strategically defeating al-Qa'ida as a terrorist threat. The killing of a number of senior operatives including its leader, Osama bin Laden, provides a hopeful indication that the threat posed by AQ Central (the core al-Qa'ida group concentrated in Afghanistan/Pakistan) may be weakening. However, despite the elimination of many key al-Qa'ida members, its adaptive nature and ability to launch operations – including Afghanistan, Pakistan, and al-Qa'ida 'franchises' in countries like Yemen– has lead the Office of the Director of National Intelligence (ODNI) to categorize this violent group as an unacceptable risk to national security. Additionally, the risks posed by self-radicalizing groups and individuals including right-wing terrorists have become more apparent, further boosting the need for more accurate and reliable assessment.

Governments have responded to these challenges by applying techniques grounded in the intelligence-led policing model (ILP) to assess terrorism threats (Lemieux, 2006; Lemieux, 2008a; Lemieux, 2008b; Verfaille and Beken, 2008). Threat assessment is intelligence-driven, aims to provide a comprehensive understanding of the nature of a given threat, to communicate the level of seriousness of that threat to decision-makers and, in the case of open source releases, to the general public. The ultimate purpose of a threat assessment is to identify warning signs, generate potential perpetrator profiles, and have preventive measures in place to deter potential threats from becoming operational. The most notable open source documents released by the US are assessments published by the ODNI, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and DHS. Foreign government agencies including the RCMP, BFP, and the United Kingdom's Security Service (commonly known as MI5) also have generated terrorism threat assessments that are publicly available. Similarly, think tanks such as the Rand Corporation have published reports on risks and threats related to terrorist groups or activities (Jackson et al., 2005; Willis et al., 2005). Reliance on these tools for CT domestically and internationally raises important concerns about the conceptual reliability of terrorism threat assessment methodologies to accurately generate situational awareness and to be effectively integrated into strategic decision-making from the perspective of law enforcement.

Published data and our own experience strongly indicates that intelligence-driven strategies require consolidating the physical, informational, and behavioral sciences into logical, cohesive overlays or patterns that can be applied to human

terrain data (e.g., individuals and groups in an operational environment). That is, situational awareness of real world phenomena within specified temporal and spatial domains (e.g., perception of environmental elements) forms a common intelligence picture of potential adversarial threats to be used by law enforcement agencies (Smith, Demphousse and Roberts, 2011). It provides the 'what to report' as well as the 'what if' and 'so what' for intelligence data, and is a foundational component of counterterrorism that is grounded in actionable and credible subject matter knowledge. Such analysis inevitably is based on the fusion of a large accumulation of data and experience. To meet the precipitating challenges of transforming first responders into first preventers, the 9/11 Commission recommended developing fusion centers to adapt the ILP concept to counterterrorism (National Commission on Terrorist Attacks Upon the United States, 2010). Drawing on its prior experience with ILP to identify chronic high-rate criminal offenders and other recurring problems, the UK similarly has endorsed an intelligence-driven model for law enforcement engagement in counterterrorism, particularly integrating ILP with community-oriented policing to thwart homegrown terrorists (Riley et al., 2005; Clark and Newman, 2007).

Not surprisingly, generating valid and reliable risk assessments that are actionable to counter adversarial behaviors is a challenging endeavor. Terrorists are not homogeneous. They differ widely in terms of capabilities; motivations; decision-making information, skills, and processes; and organizational or personal psychology. Because political violence in general, and terrorism in particular, is not the exclusive domain of a single academic discipline, building actionable knowledge and understanding requires an interdisciplinary approach to overcome existing conceptual and methodological limitations. This is particularly true when it comes to integrating mathematical formulas and using risk theory. Table 1 presents current methodological approaches used in assessing terrorist risk and their associated shortcomings.

Table 1: Current methods use in Terrorism threat/risk assessments and their limitations

Methods	Limitations
Qualitative methods that provide descriptive analysis for tactical/operational and/or strategic decision-making	These methods lack rigor and provide only loose conceptualization/operationalization
The Delphi method to weigh terrorist attributes and rank order them for prioritization purposes	Method results provide subjective appraisals that does not account for error or uncertainty
Probability models to quantify estimated risk based on some combination of threat, vulnerability, and consequence	Approaches result in partial model parameterization and deficient data quality

Unfortunately, there is no 'gold standard' (i.e., best practice) that has achieved universal acceptance despite some crossover of common elements for risk assessment. For instance, the U.S. General Accountability Office (GAO) published a report in the aftermath of 9/11 events asserting that a "good risk management approach" should include three main elements: (1) a threat assessment; (2) a vulnerability assessment; and (3) a criticality assessment (U.S. Government Accountability Office, 2001). According to the GAO, a threat assessment identifies and evaluates threats based on various factors including capability and intentions, as well as the potential lethality of an attack. A vulnerability assessment refers to a process that identifies weaknesses that may be exploited by terrorists and suggests options to eliminate or mitigate those weaknesses. A criticality assessment identifies and evaluates an organization's assets based on the importance of its mission, the group of people at risk, or the significance of a structure.

Similarly, a Rand Corporation report asserted that a terrorist risk assessment should be based on an analytic process (e.g., quantitative) relying on three central factors to determine terrorism risk: (1) *threat* measured as the probability that a specific target is attacked in a specific way during a specified period; (2) *vulnerability* measured as the probability that damage [i.e., fatalities, injuries, property damage, etc.] could occur according to a given a threat; and (3) *consequences* measured as the magnitude and type of damage resulting given a successful terrorist attack. Using the Rand approach, risk is a function of threat, vulnerability, and consequences (Willis et al., 2005). The report describes two approaches for estimating terrorism risk: (1) simple risk indicators that explore the link between population-based indicators and terrorism risk and (2) event-based models built upon relatively detailed analysis of consequences from specific attack scenarios.

Homeland Security Presidential Directives (HSPD) -10, - 18, and -22, recognize the need for systematic, science-based, terrorism risk assessments that inform strategic planning and resource prioritization. To address this need, DHS S&T developed a set of Terrorism Risk Assessments: Bioterrorism Risk Assessment [BTRA], Chemical Terrorism Risk Assessment [CTRA], and Integrated Chemical, Biological, Radiological and Nuclear Terrorism Risk Assessment [ITRA]. In addition, the Risk Assessment Process to Inform Decision-making (RAPID), in support of the DHS Policy for Integrated Risk Management (May 27, 2010), provides an all-hazards risk analysis by incorporating the information from all of these TRAs and addresses additional risks such as those from natural disasters and other threats. The TRAs mirror aspects of the Rand approach described above and are help prioritize protecting critical infrastructure against terrorist attacks. The TRAs are probabilistic risk assessments that integrate the expert judgments of the

intelligence and law enforcement communities with those from the scientific, medical, and public health communities. This approach is based on the following formula:

$$\text{Risk} = f(\text{Threat} \times \text{Vulnerability} \times \text{Consequences}) \quad \text{[Eq. 1]}$$

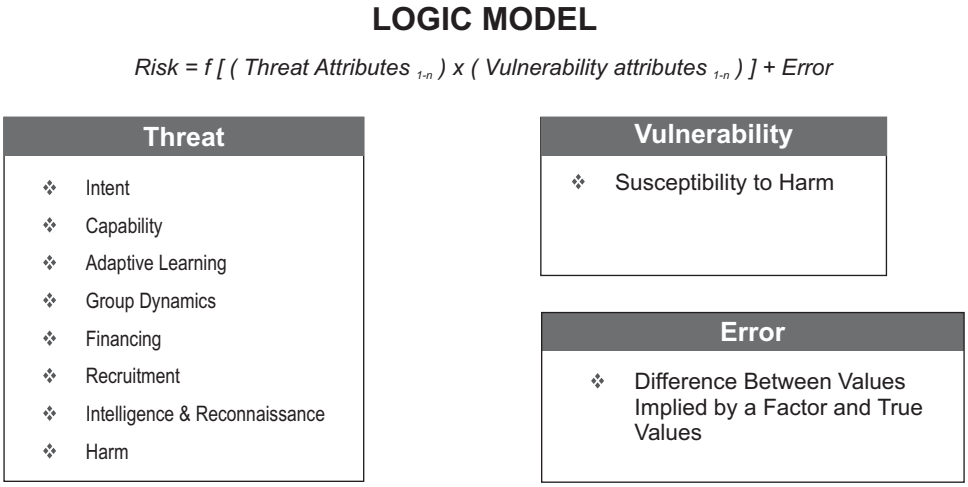
As Cox notes, several conceptual and methodological challenges arise when one attempts to directly assess threat probabilities for the actions of intelligent antagonists versus modeling how they adaptively pursue their goals in light of available information and experience (Cox, 2008). First, estimates have a very high degree of unavoidable uncertainty due to the relatively rare nature of terrorism threats and/or the scarcity of data. A number of studies have demonstrated that estimating the probabilities of high-impact, low-frequency events is extremely difficult and often produces highly subjective assessments (Krimsky and Golding, 1992; Weber, Blais, and Betz, 2002). Illustrating the imprecision of such subjective appraisals, a study concluded that assuming an annual worldwide death rate from international terrorism of approximately 1,000 victims/year (based on U.S. Department of State estimates), the lifetime probability that a person will be killed by terrorists is about 1:75,000 which, he points out, is about the same likelihood that one would die from the impact of an asteroid colliding with the Earth (Mueller, 2007). In other words, risk models based on probability produce an excessive level of uncertainty. Second, methodological issues are associated with the structure of the formula and its conceptual articulation. These include: (1) the failure to adjust for correlations among components (e.g. measures of damages and consequences); and (2) potential non-additivity of estimated risks. Third, there are inherent uncertainties and randomness associated with terrorism threats due to several factors: (1) terrorist entities are clandestine, closed systems making credible and timely acquisition of information problematic (Willis et al., 2005; Aust, 2009; Giorgio, 2003); (2) terrorism campaigns are dynamic (i.e., they occur over time with corresponding shifts in counterterrorism efforts and adversarial behaviors) (Cronin, 2009; Bjorgo and Horgan, 2009); and (3) law enforcement officials, especially at the state and local levels (due to the structure of the justice system), play a significant role in countering terrorism within the US which makes the situational awareness of those individuals critical in preventing and mitigating attacks (Riley et al. 2005; Carter and Carter, 2009).

Alternative Approach in Conceptualizing and Developing Logic Model of Terrorist Risk Assessment

When one takes these methodological and conceptual considerations into account, three factors must be addressed in order to design, parameterize, and interpret a new evidence-based assessment of terrorism risks: *threat, vulnerability* and *error/randomness*. On the threat dimension, the assessment must measure the *intent*, *capability*, and *harm* of a given terrorist group or 'lone wolf' actor within the context of a terrorist campaign. On the vulnerability dimension, the analysis must measure the *reliability and effectiveness of existing counter-measures*. Finally, it is essential to provide an *estimation of errors*. This last element is crucial because it quantifies and bounds the randomness of errors and information about the stability of predictions as well as the level of uncertainty attributable to the model. The following equation illustrates the conceptualization we propose:

$$Risk = f\left[\left(Threat\ attributes_{1\text{-}n} \right) x \left(Vulnerability\ attributes_{1\text{-}n} \right) \right] + Error \qquad [\text{Eq. 2}]$$

The threat attributes component or dimension that 'drives' risk requires specification and operationalization of multiple indicators in order to quantify threats to be linked through mathematical equations. Similarly, the vulnerability dimension of Eq.2 requires explicit metrics for inclusion in the equation. The error term quantifies the difference between values implied by a factor and the true values of the quantity being calculated. In the next section, we present the logic model that underlies our proposed algorithm-based this second equation.



Historically, groups (as opposed to 'lone wolf' actors) predominate in conducting terrorist campaigns. As a result, we opt to focus on group-centric modeling of adversarial behavior and our logic model is grounded in the following general premises:

- Risk assessment should seek robust risk estimators that account for uncertainty about terrorism risk;
- Algorithm-based assessments can serve both operational and strategic purposes by providing realistic threat and vulnerability measures;
- Analyzing these complex dynamic interactions, many of which are not well understood, requires simplification; and
- Too much simplification produces results, which may be useless or misleading.

Given these premises, we turn to describing how the key components of the model are conceptualized.

Threat represents the first of the two dimensions included in Eq. 2 that determine risk. It can be conceptualized as encompassing intent, capability; adaptive learning; group dynamics; financing; recruitment; intelligence and reconnaissance; and harm. For example, the underlying capability and intent as well as adaptive learning ability of a group can affect the persistence of terrorist campaigns, especially adaptation to CT measures (Cronin, 2009; Bjorgo and Horgan, 2009). As a result, when the components of the logic model are taken as a whole, the elements of threat component represent necessary but not sufficient conditions for terrorism to pose a risk. Each element of threat is defined below.

Intent refers to an opponent's ideology, motivations and desire to engage in adversarial behaviors and is a necessary but not sufficient condition for threat materialization (Schmid and Jongman, 2005; Crenshaw, 2000). Ideology refers to the underlying belief system (i.e., attitude structure for interpreting phenomena) that can explain and/or motivate action. Two paradigms, *prophetic* and *dialectic*, serve as proxies for motivation for terrorism. Religious and white supremacist groups commonly are categorized into the prophetic paradigm; the Aum Shinrikyo sect provides an example of prophetic terrorism. Left-wing and nationalist terrorist groups tend to be categorized into the dialectic paradigm; the Irish Republican Army (IRA) and the Quebec Liberation Front (FLQ) are examples. In parallel, radicalization processes – both religiously and non-religiously inspired – shape the dynamics of domestic and international terrorism (Jones, 2008; Horgan, 2005). A number of recent studies find individuals must progress sufficiently through a process of radicalization to acquire both the motivation and ability to support and, ultimately, to commit acts of goal - directed political violence. Finally, a terrorist

group must express directly or indirectly its intention to carry out violent actions against an entity. Each of these components of intent needs to be represented formally in an objectives hierarchy.

155*Capability* refers to the scientific/technical expertise, organization structure, and operation financing (e.g., tactics, weaponry) that a terrorist group possesses. Since 1968, terrorists have employed a wide range of weapons, from knives to assault rifles to toxic chemicals. Weapons in a general sense, constitute a logical and straightforward requirement, access to external weapon sources and/or unconventional weapons add another degree of complexity to this requirement. Indeed, it appears that as groups expand their activities, the reliability of weapon supplies becomes a more important operational requirement than simply having access to large weapons stockpiles. The array of potential threats encompasses chemical, biological, radiological, and nuclear terrorism, as well as conventional explosives, which remain the most common weapons used by terrorist groups.

Examples of possible attack scenarios include release of chemical warfare agents or toxic industrial chemicals in confined spaces; aerosol releases of bacterial, viral, or toxin agents in a building environment; the deliberate release of non-fissile nuclear material using a radiological dispersion device (RDD), commonly called 'dirty bombs', to contaminate a major port facility; the detonation of an improvised nuclear device (IND); or the use of conventional explosives to produce mass casualties and/or infrastructure destruction. Each scenario has different scientific and engineering barriers, especially acquisition of sufficient materials and delivery/use at a target, which affect an adversary's capabilities to execute the scenario. Those factors that influence the ability to attack are impacted by the choice of weapons, delivery technologies, time frame, and feasible target set. For example, although most microorganisms that cause disease or produce toxins (i.e., viruses, bacteria, fungal spores, and toxins) can be used as biological weapons, some are more likely candidates for use because they are extremely infectious and exhibit high mortality or debilitating mortality rates (Lane, Montagne and Fauci, 2001; Reshetin, and Regens, 2003). Similarly, an IND, unlike a RDD, requires sufficient fissile material (^{235}U or ^{239}Pu) and the proper design configuration to achieve criticality (Regens and Gunter, 2010; Regens, Gunter and Beebe, 2007). Comparable technical constraints apply to chemical terrorism (Regens et al., in press) or, for that matter, in the case of conventional explosives (Peleg et al. 2011). The increased likelihood, and perhaps inevitability, that terrorists will attempt to use weapons of mass destruction (WMDs) or weapons of mass effect (WMEs) is a core assumption of current assessments of the threat posed to homeland security by terrorism (Lane, Montagne and Fauci, 2001; Hoffman, 2006). The employment of Improvised Explosive Devices (IEDs) and other more common modes of attack further complicate the threat environment. However, the use of complex weaponry requires some level of sophistication and expertise.

Adaptive learning refers to the ability to hone expertise through learning from experience and emulating the successful behavior of others. Terrorist groups embody this attribute because they need to provide their members with the technical skills to conduct attacks successfully (e.g., bomb making, weapon handling, and even operational security techniques). Addressing adversary adaptation requires understanding the ways terrorist groups can respond to new defensive or other changes. They have a variety of options, each with distinct direct and indirect risk effects. For example, al-Qa'ida operatives are known to be highly adaptive in learning from past successes and failures (Springer, Regens and Edger, 2009). Relationships with other like-minded groups, possibly as an investment for future cooperation or help, also can be a way to gain "supplemental" expertise and/or training (Jackson et al., 2005). In addition to formal camps that require a secure operational base, the Internet and social media technology have become critical mechanisms for adaptive learning.

Group dynamics refers to the structural and leadership characteristics of social organizations. Command and control is the group dynamic mechanism that terrorist groups use to plan, coordinate, and execute their attacks. Command and control is a relatively consistent requirement across all terrorist groups, despite varying degrees of capabilities. The effectiveness of the attacks that a terrorist group might be capable of launching depends much on the structure of its organization. The less centralized and hierarchical, the more resilient the organization will be to CT action. A more elusive and resilient type of network architecture has no hub, but consists simply of a set of terrorist cells, which may comprise one or more individuals. For an emergent network under constant pressure from international CT forces, the types of attacks that can be attempted will be constrained by available resources (Jackson et al., 2005). For example, high loss scenarios may be attractive to AQ, but they may also be especially hard to execute under pressure. Also, the IRA campaign provides illustrations of the effectiveness of heightening security and cutting off supplies of armaments in reducing the options for terrorist action. Terrorist groups tend to coalesce around charismatic individuals who attract and inspire supporters. Therefore, leadership in this context plays a more cohesive than operational role, and we would expect that the most adversarial terrorists groups have fairly charismatic leaders like bin Laden (Springer, Regens and Edger, 2009).

Financing refers to the ways terrorist groups acquire financial resources. As such, money is best considered an operational and strategic tool; financing activities can be categorized as being (1) operational or (2) strategic (Ehrenfeld 2003; Warde, 2008). Short-term funding sources are usually exploited for operational purposes and represent a flexible "means-end financing". Operational financing is largely task-oriented and does not require sophisticated funding sources to support disorganized local entities or decentralized structures. Strategic financing aims to

support the long-term activities. According to Hoffman (2006), financing is a key element in ensuring the endurance of terrorist groups in part because they successfully acquire the loyalty of community members. Moreover, recent studies emphasize the function of voluntary organizations (i.e., 'club' model) as efficient providers of local public goods in the face of government failure to do so (Berman and Laitin, 2008). These "violent clubs" act as social movements and possess sufficient financial resources and a base of supporters within the community to function as alternatives to formal governmental institutions (e.g., Hamas, Hezbollah).

Recruitment refers to the processes for attracting new members both to grow in strength and to replenish losses and defections. Recruitment can be so important that one study of left-wing terrorism in Italy from 1970 to 1983 found that groups conducted increasingly lethal attacks, in part, to gain more recruits (Della Porta, 1995a, 1995b).

Intelligence and reconnaissance/casing refers to the basic skills in information collection and analysis that terrorists need to identify a potential target and plan/execute a method of attack, which engenders a desired response from its intended audience. Logically, we expect that the degree to which terrorist groups need intelligence will be directly related to the sophistication of the planned attack. Intelligence and reconnaissance includes activities designed to establish an accurate understanding of the local operating environment and the effect of an attack on their adversaries.

Harm refers to the severity of the event (e.g., deaths, injuries, psychological damage, level of critical infrastructure destruction, etc.) and its potential societal impacts (e.g., economic costs, impact on trust in government, etc.). That is, harm is a measure of a terrorism event's consequences.

Vulnerability represents the second of the two dimensions included in Eq. 2 that determines risk. Assessment of vulnerability is mainly related to the evaluation of the counter-measures. Most studies have looked at situational prevention and physical protection focusing on deterrence, preparedness, and response to mitigate consequences. The Department of Homeland Security defines vulnerability as a "physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard". For the purpose of this study, the vulnerability characteristics of a target will be drawn from the information contained in the database for each incident (if available). Factors such as location, accessibility, and the nature of the target (hard or soft) can explain the fluctuation of terrorist attacks.

Error is the third component that our logic model incorporates. Estimates of risk generated using indicators of threat and vulnerability are inevitability uncertain. For example, we know terrorists may build IEDs and vulnerabilities to IEDs exist under some scenarios. That is, each dimension is necessary and some combination of the two dimensions is a sufficient condition for risk. However, because we lack perfect information, some error in likelihood estimates is inherent in our predictions. Moreover, even 'known' information is subject to uncertainty, thereby introducing error into our estimates of risk.

The ***error term*** in Eq. 2 refers to a statistical estimator that quantifies the difference between values implied by a factor and the true values of the quantity being calculated. Mean Squared Error (MSE) plays a role of "risk estimator" within the equation, corresponding to the expected value of the squared error loss. In the formula to assess terrorism risk, the MSE is used to determine whether the risk model does not fit the data well and/or whether removing or modifying factors can simplify the model.

Suggested Methodology

Modeling adversarial threats has the potential to inform probabilistic estimates of adaptive attack behavior and aid law enforcement in the design and selection of anti-terrorism countermeasures. The overall strategy for applying the Logic Model outlined in the preceding section involves building on the broader literature, existing models, and our own prior work to: (1) parameterize the "theoretical model" based on open source data supplemented by indicators from the broader literature as well as our prior studies; (2) parameterize existing law enforcement practical models; (3) estimate threats using historical data to compare models' output; (4) specify an integrated theoretical model that captures key parameters with the greatest predictive power in the practical models used by the law enforcement existing models; (5) verify the predictive power of the integrated algorithm-based model; and (6) interpret the findings and develop desktop application that captures structured, encryptable data on terrorist events. The methodology must follow a series of step in order to produce a robust modelization

First, database architecture should be designed to include data entry protocols providing randomized checks of data integrity to review values entered and correct invalid information prior to and subsequent to populating the database, in order to ensure quality control data entry. The database management architecture should also include procedures for data archiving. Completion of this task, which includes a protocol for ongoing database management, is necessary for modeling and advanced data analysis. In parallel to designing the database, it is also crucial to design data entry protocols for all data to populate the relational databases. Protocols should be developed and implemented to provide randomized checks of

data integrity to review values entered and correct invalid information prior and subsequent to populating the database. This task is critical because standardized procedures are necessary to ensure consistent, replicable techniques are used for database construction.

Second, a data set should be created. This task is crucial because it leads to the development of the theoretical terrorism risk assessment model. Task 3 involves four sub-tasks: (1) collecting data from public sources; (2) applying geographic identifiers (x, y coordinates) to those data; (3) populating the geo-referenced database; and (4) analyzing the data set with regression techniques and other statistical tools. As main source of data, the Global Terrorism Database can be used. GTD is an open-source database including information on terrorist events around the world from 1970 through 2010, with additional annual updates planned for the future. Unlike many other event databases, the GTD includes systematic data on domestic as well as transnational and international terrorist incidents that have occurred during this time period and now includes more than 98,000 incidents. For each GTD incident, information is available on the date and location of the incident, the weapons used and nature of the target, the number of casualties, and – when identifiable – the group or individual responsible. The National Consortium for the Study of Terrorism and Responses to Terrorism (START, a DHS academic center of excellence) maintains this database.

Another database that include open source data available from the New America Foundation and Syracuse University's Maxwell School of Public Policy database of post-9/11 Americans or U.S. residents convicted or charged of some form of jihadist terrorist activity, as well as the cases of those American citizens who have traveled overseas to join a terrorist group along with details of the alleged plots. The New America Foundation/Syracuse University data can be used to supplement the GTD.

All data should be linked to geographic identifiers and geo-referenced to support modeling the spatial component of terrorist threat. Geo coded data on terrorist attacks can be useful to assess the geographical scopes of terrorism activities. It can also help identifying concentration areas where some terrorist activity takes place. Data will also be analyzed using time-referenced data in order to better understand the relation between fluctuation of attacks (dependent variable) and threat/vulnerability characteristics (independent variables) over the time. Both spatial and temporal analyses will provide critical results regarding the specificities of some groups or target characteristics that are more susceptible to fluctuation according to time or space.

Finally, a first round of analysis must be conducted to estimate the specification of the theoretical model in order to analyze the influence of the indicators outlined in

the logic model summarized above. This procedure provide an opportunity to estimate the reliability of the theoretical model, test for autocorrelation and multicolinearity problems, and identify variables that need to be removed from the model.

Third, the accuracy and reliability of existing threat assessment models should be tested against the database described in this section. Testing these "practical models" from law enforcement can help to identify additional relevant concepts/variables to be included in Eq. 2. This stage consists of: (1) populate models using GTD values; (2) estimate terrorist threat predictions; and (3) interpret model results. For example, threat assessment models developed by the Royal Canadian Mounted Police and the Belgian Federal Police can represents an excellent source of data for comparisons.[1] This third phase involves estimating terrorism risk using the law enforcement models. Each of the models selected for evaluation can be used separately to generate terrorism threat predictions using historical data. Finally, this phase involves interpreting the law enforcement model results. Qualitative appraisals and statistical analysis procedures should be used to identify key predictors from both models. Potential measures may include residual errors, coefficient estimates, coefficient standard errors, and goodness of fit measures. In essence, which parameters from which models are most accurate in predicting those historical events?

The fourth phase requires the elaboration of an integrated algorithm-based risk model, based on a system of mathematical equations, which incorporates the key parameters identified above combined with subject matter expert judgments and input from the law enforcement community. It is crucial that the model's system of equations integrates and weights appropriately each of the three elements described in the logic model (e.g., *threat*, *vulnerability*, and *error*).

Finally, the last phase is about populating the Integrated Algorithm-based Model and Estimate Terrorism Risk. More precisely populating the parameters for the algorithm-based model specified before, drawing on the GTD and supplemented by the law enforcement information for initial parameterization. The model can then be re-specified and calibrate by utilizing a random sample of terrorism incidents from the database developed. Finally , the performance of this new terrorism risk

[1]The RCMP developed a model called "*Sleipnir*" for national threat assessments on terrorism and criminal extremism. The *Sleipnir* model allowed the RCMP to set priorities in its fight against terrorist groups. To date, the BFP's Integrated Police Operation Directorate and its Strategic Analysis Service have identified more than 30 recurrent or emerging security problems against which police must take action, including terrorism. However, only certain elements of terrorists' capacity were included in the threat assessment model.

model (Equation 2) must be compared to the existing risk model developed by Department of Homeland Security (Equation1) to understand and underscore the conceptual contribution to the field as well as its application to situational awareness and strategic decision-making for law enforcement agencies.

Conclusion

The application of algorithm model to terrorism risk assessment can help to understand better pattern of violent groups over a period of time. This approach can serve both operational and strategic purpose by (1) providing realistic measures to investigators and intelligence officers on threat and vulnerability characteristics and (2) using individual terrorism group risk factors to help decision-makers to identify strategic priorities as wells as appropriate tactics to reduce vulnerabilities and mitigate threats. However, this model does not predict terrorism attacks neither it provides a crystal ball to analysts. Another limitation related to algorithm-based approach is the availability of significant amount of data in order to generate reliable models. The application of robust risk analysis can help law enforcement agencies to prioritize groups that present the most serious security risks, allocate resource efficiently, elaborate more effective counter-terrorism strategies and tactics thereby increasing safety for communities.

Reference

Aust, S. (2009). *Baader-Meinhoff.* Translated by A. Bell. New York: Oxford University Press.

Berman, E. and D. D. Laitin (2008). *Religion, Terrorism and Public Goods: Testing the Club Model*. NBER Working Papers. 13725, National Bureau of Economic Research.

Bjorgo, T. and J. Horgan (Eds) (2009). *Leaving Terrorism Behind*. London: Routledge.

Carter, D.L. and J.G. Carter (2005). Intelligence-led policing. *Criminal Justice Policy Review* 20: 310-325.

Clarke, R.V. and G.R. Newman (2007). Police and Prevention of Terrorism. *Policing* 1 (1): 9-20.

Cox, L. A. Jr, (2008). Some Limitations of Risk = Threat × Vulnerability × Consequence for Risk Analysis of Terrorist Attacks. *Risk Analysis*, 28: 1749–1761.

Crenshaw, M. (2000). The psychology of terrorism. *Political Psychology* 21: 405-420.

Cronin, A.K. (2009). *How Terrorism Ends*. Princeton, NJ: Princeton University Press.

Della Porta, D. (1995a) *Social Movements and the State: Thoughts on the Policing of Protest*. European University Institute.

Della Porta, D. (1995b). Left-Wing Terrorism in Italy, in Martha Crenshaw (ed.) *Terrorism in Context,* pp. 134-157. State College, Pa.: Pennsylvania State University Press.

Ehrenfeld, R. (2003). *Funding Evil: How Terrorism is Financed and How to Stop it*. Santa Monica: Bonus Books.

George R.Z. and J.B. Bruce (eds.) (2008). *Analyzing Intelligence.* Washington: Georgetown University Press.

Giorgio (2003). *Memoirs of an Italian Terrorist.* translator A. Shugaar. New York: Carroll & Graf.

Heuer, R.J. Jr. (1999). *Psychology of Intelligence Analysis*. McLean, VA: Central Intelligence Agency, Center for Study of Intelligence.

Hoffman, B. (2006). *Inside Terrorism.* New York: Columbia University Press.

Horgan, J. (2005). *The Psychology of Terrorism*. London: Routledge.

Jackson, B. et al. (2005). *Aptitude for destruction: organizational learning in terrorist groups and its implications for combating terrorism.* Santa Monica: Rand Corporation.

Jones, J.W. (2008). *Blood That Cries Out From the Earth*. New York: Oxford University Press.

Krimsky, S. and D. Golding (1992). *Social theories of risk*. Westport, CT: Praeger-Greenwood.

Lane, H.C., J. L. Montagne and A. S. Fauci (2001). Bioterrorism. *National Medicine* 7:1271-1273.

Lemieux, F. (2006). *Norms and Practices in Criminal Intelligence: An International Comparison*. Ste-Foy: Laval University Press.

Lemieux, F. (2008a). Information Technology in Criminal Intelligence Services: A Comparative Perspective. in Leman-Langlois, S. (Ed.) *Technocrime*, pp. 139-168. Columpton, UK, Willan Publishing.

Lemieux, F. (2008b). A Cross Cultural Comparison of Intelligence Led Policing, in Williamson, T. (Ed.) The Handbook of Knowledge Based Policing: Current Conceptions and Future Directions, pp. 221-240. Chichester, U.K., Wiley & Sons.

Mueller, J. (2007). Reacting to Terrorism: Probabilities, Consequences, and the Persistence of Fear. *Paper presented at the annual meeting of the International Studies Association 48th Annual Convention, Hilton Chicago* Chicago, IL, USA, Feb. 28.

National Commission on Terrorist Attacks Upon the United States (2010). *The 9/11 Commission Report*. Washington: U.S. Government Printing Office.

Peleg, K., J.L. Regens, J.T. Gunter and D.H. Jaffe (2011). The normalization of terror. *Disasters* 35: 268-283.

Regens, J.L. and J.T. Gunter (2010). Predicting the magnitude and spatial distribution of potentially exposed populations during IND and RDD terrorism incidents. *Human & Ecological Risk Assessment* 16: 236-250.

Regens, J.L., J.T. Gunter and C.E. Beebe (2007). Estimating total effective dose equivalents from terrorist use of radiological dispersion devices. *Human & Ecological Risk Assessment* 13: 929-945.

Regens, J.L., J.T. Gunter, M. Amin, A. Nowakowski & H. Navaz (in press). Parameterizing potential exposure to HD using mixed model regression" *Human & Eco Risk Assess*.

Reshetin, V.P. and J.L. Regens (2003). Simulation modeling of Anthrax spore dispersion in a bioterrorism incident. *Risk Analysis* 23: 1135-1145.

Riley, K.J., G.F. Treverton, J.M. Wilson and L.M. Davis (2005). *State and Local Intelligence in the War on Terrorism*. Santa Monica: RAND.

Schmid, A.P. and A.J. Jongman (2005). *Political Terrorism.* Amsterdam: North Holland Publishing.

Smith, B., K. Demphousse, and P. Roberts (2011). *Pre-Incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic and Temporal Patterns of Preparatory Conduct.* Washington D.C.: U.S. Department of Justice.

Springer, D.S., J.L. Regens and D.N. Edger (2009). *Islamic Radicalism and Global Jihad*. Washington: Georgetown University Press.

U.S. Government Accountability Office (2001). *Homeland Security. Key Elements of Risk Management Approach*.

Verfaille, K. and T. V. Beken (2008). Proactive policing and the assessment of organized crime. *Policing: An International Journal of Police Strategies & Management*, 31(4): 534 – 552.

Warde, I. (2008). *The Price of Fear.* Los Angeles: University of California Press.

Weber, E. U., A. R. Blais, and N. Betz (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making* 15: 1-28.

Willis, H. et al. (2005). *Estimating Terrorism Risk*. Santa Monica, Rand Corporation.

The author Frederic Lemieux is Professor and Program Director of the bachelor's degree in Police Science and master's degree in Security and Safety Leadership at The George Washington University. Dr. Lemieux has numerous publications in English and French on terrorism financing, best practices in strategic intelligence, militarization of the intelligence community, and international police cooperation. He spearheaded several international research projects on intelligence-led policing in collaboration with the Royal Canadian Mounted Police; Serious Organized Crime Agency (United Kingdom); Drug Enforcement Administration; Belgium Federal Police; Europol (Netherlands); Interpol (France); OCTRIS (France); Colombian National Police and Department of Administrative Security (DAS); Venezuela National Police; Singapore Police Force; Australian Federal Police and Australian Crime Commission; NATO (Europe); and Geneva and Lausanne canton police forces (Switzerland). Prof. Lemieux can be reached at flemieux@gwu.edu.

The author James L. Regens holds the Edward E. and Helen T. Bartlett Foundation Chair and is founding Director of the Center for Biosecurity Research at the University of Oklahoma Health Sciences Center. Dr. Regens has served in policy and analytical positions in government and national laboratories and is a member of the Council on Foreign Relations. He has authored or co-authored over 200 scientific and technical publications including articles in journals such as Proceedings of the National Academy of Sciences, Risk Analysis, and Human & Ecological Risk Assessment as well as eight books. Dr. Regens can be reached at Larry-Regens@ouhsc.edu.

Terrorism Investigation in Pakistan: Perceptions and Realities of Frontline Police

Fasihuddin (PSP)

Abstract

This paper analyses the constraints faced by frontline police in Pakistan when undertaking investigations into terrorism cases. The complexity of this issue is further compounded by a serious lack of empirical research on terrorism investigations and its management in Pakistan. Hence, this study used a purposive sample based on research interviews with police officials in the province of Khyber Pakhtunkhwa (KP) in Pakistan where a significant number of terrorist cases occur. The results of this study present an extremely depressing picture about the multiplicity of serious constraints faced by police at the forefront in the war on terrorism in Pakistan.

Keywords

Terrorism, Investigation, Constraints, Khyber Pakhtunkhwa (KP), Police, Prosecution, Prevention, Research.

Introduction

Despite the fact that Pakistan joined the war on terror in 2001 and earned a name for herself as the frontline state against terrorism and extremism, she couldn't develop a meaningful and effective counter-terrorism policy at the national level. Pakistan's policy-makers terribly failed to create a consensus on a national strategy. Police have become the prime targets as far as the militant activities are concerned. The counter-terrorism measures of the police remain in-effective. The abysmally poor performance of the police in preventing and investigating the terrorist incidents is a hot topic for the media and public in Pakistan. In spite of this media spotlight the investigation of terrorism is a relatively ignored and neglected area by researchers as well as the law enforcement officials in Pakistan. Therefore, the focus of this paper is to establish for the first time a type of research baseline about the major constraints and management flaws involved in the investigation of terrorism cases, particularly in the KPK province of Pakistan.

Literature Review

Finding relevant literature on terrorism with reference to Pakistan is a difficult task. Despite the availability of enormous literature on terrorism, the actual investigation of terrorism cases is a missing link in literature. Bensinger (2010) argues that the challenge of terrorism in a free society strains the delicate balance between security and individual civil liberties. He describes the structure of law-enforcement in post 9/11 Germany and various multilateral and unilateral initiatives

taken by Germany in the war against terror. It can be inferred from his paper that the German law-enforcement has taken very effective preemptive measures to stop terrorists from materializing their plans. However, Bensinger did not mention anything about investigation of terrorism. The same is true for much of the international research on terrorism.

In a previously published article, the author himself acknowledges the fact that there was a little contribution towards investigation management by researchers (Fasihuddin, 2010). Along with constraints in data, he identifies various constraints in investigation in terrorist cases in Pakistan. The on-scene constraints identified were; public anger, dis-orderliness, commotions, media race for early coverage and too many cameras at the crime scene. The most surprising point that the author raised was the effect of the new police reforms on investigation in Pakistan. Under the new police law, Police Order 2002, the police wings were separated into prevention and investigation. The author laments that these reforms brought the worst day for police investigation. It was pointed out that the police officers avoid being placed in investigation wing. They try to secure posting in the prevention wing. Most of the problems the author identifies are not something which cannot be tackled with.

O'Connor (2010) stresses the real challenge of terrorism lies in its political nature. To him, terrorists are the offenders who see themselves as celebrities. They want media attention drawn to their case, and in particular, to the justice of their cause. Simultaneously, they want attention drawn to injustices inflicted upon them by authorities. O'Connor concludes that these factors along with many others make up the real challenge of terrorism investigation. Although very thorough and focused, O'Connor's paper focuses almost entirely on proactive, preemptive investigation measures (in the US), e.g. record checks and interviewing, terrorism database and watch list, foreign intelligence surveillance, and the role of classified information procedure. However, as mentioned earlier, the real trouble for law enforcement in Pakistan is in the area of reactive investigations.

O'Connell (2008) uses a 'Chess Master's Game' metaphor to suggest police need to be strategic and tactical in their approach towards terrorism cases. He emphasizes the need for police to know that "*an act of terrorism, e.g. a bomb blast or a suicide attack, is simply an opening gambit by a relatively unsophisticated opponent, or one with a continuing and escalating array of moves by particularly competent and dangerous adversary*." He concludes that only by thinking in a Chess Master's Game way, can the police properly categorize threat levels and properly align and utilize their resources against terrorists. The acts of terrorism in Pakistan are a continuing series of moves by the competent and dangerous terrorists. The law enforcement, however, seems to ignore this fact and search for the potential roots in

a group of crude opponents. Further, there have been random measures taken to counter terrorism in Pakistan. The measures taken by law enforcement agencies do not seem to have been adopted in any of Chess Master's Game way; in other words, no strategic policy to counter terrorism. It should be kept in mind that plenty of the literature available on terrorism is mostly journalistic and political in nature, and rarely empirical and based on true case files. Police and intelligence record is usually not easily available.

It is cannot be emphasized enough that most of the complex processes involved in radicalization and motivation of the terrorists are beyond the reach of any police work and other law-enforcement agencies. Rather conclusions are based on educated guesses, public perceptions, police files of arrested terrorists or suspects and, at times, leakages from or surveillance of militant organizations and their workers. Academics too have very limited approach to the official record and again the complex processes of prevention, investigation, intelligence-gathering and prosecution of terrorist cases, especially of the high-profile incidents where a variety of military and civil law-enforcement agencies are involved. This is perhaps the only reason why we don't have a good deal of literature on policing, investigation and prosecution of terrorism incidents, like we have about drugs, sexual abuses, human-trafficking or murder. It is because of this lack of knowledge and inaccessibility to the inside information that books and other material on terrorism contain more political, psychological, religious and economic discussions on terrorism, counter-terrorism and war on terror than on the real issue of policing terrorism. For example, Guiora, N. Amos in his books, *Global Perspectives on Counterterrorism* (2007) and *Fundamentals of Counterterrorism* (2008) hardly provides any real policing challenges in dealing with terrorism. The Turkish Institute of Police Studies (TIPS) in collaboration with the Turkish National Police (TNP) and NATO jointly held conferences on this subject and produced copious literature in many volumes, based on the selected papers and published by IOS Press in 2007 but again we don't find a good article on inside policing difficulties and the practical strategies of law-enforcement agencies how to overcome such difficulties (See, for example, NATO Science for Peace and Security Series Vol. 19, 20, 21 and 22).

The literature produced by the Turkish Institute for Security and Democracy (TISD) after the 2nd Istanbul Conference on Democracy and Global Security, however, contains some good insight. In his article, 'The Role of Police Work, Economic Development, and Political Development in Countering Terrorism', Prof. Duma (2009) rightly points out that deterrence and disruption are as important in counterterrorism, as they are in countering other forms of violent crime and criminal conspiracy. However, deterrence is unfortunately more difficult to achieve with

terrorists than with criminals, since terrorists are so often driven by dedication to a cause for which they stand ready to sacrifice their own lives. This clearly shows that in many cases prevention strategies fail for countering terrorism and investigation strategies become more important to trace and disrupt the terrorist organizations and their tactical and strategic units. Prof. Duma (2009) also rightly observes that the police are not, and in general, cannot be held responsible for addressing the underlying causes of crime. Prevention strategies generally focus on the underlying causes and facilitating factors, so again we see the importance of investigation of the terrorist cases which otherwise is a neglected area in criminological literature.

Naushad A. K. (2009) in his article on 'Suicide Bombing in the NWFP: The Need for Research and Information Collection on Human Bombers' identifies a few constraints of prevention and investigation from a police point of view, but due to scarcity of information, justifiably calls for more research in this area. However, research in the subject of suicide-bombing or terrorist attacks is, as stated above, not any easy undertaking due to the reservations, secrecy, sensitivity and limited availability of authentic information to the academics. This paper has tried to identify such grey-areas wherein a police investigator is confronted with the difficulties of dealing with terrorism incidents and which ultimately give rise to prosecution failure. Hence, public frustration, dissatisfaction, police incompetence arise along with mutual accusations amongst the various wings of the criminal justice system for being improper, non-committed, non-professional and dis-interested.

In summary, this brief literature review found that in Pakistan the investigation of terrorism is a relatively ignored and neglected area by researchers as well as the law-enforcement officials. Researchers are interested in the causes and consequences of terrorism while the law-enforcement agencies seem to be interested in preventive measures, quick fixes, hot pursuits and instant-coffee reactions. This gap in research and practice justifies the need for a further research into terrorism investigation.

Methodology

For the purpose of this research, interviews were conducted with senior police officials of the Province of KP. A total of ten (10) in-depth interviews were conducted, for two hours each. A structured interview guide was prepared. The officials were asked open ended questions related to police investigation management. Interviews were conducted with senior serving and retired police officers, especially those officers who have served in the conflict zones or have been attacked by the terrorists and have survived the attacks or who are responsible for collecting, compiling and analyzing the police crime data. Moreover, the official

record was studied and examined in senior police offices which are otherwise not published. The writer, being a senior police officer, availed the opportunity to look into some files of immense importance for this write-up. Further, the writer's personal experience and observation as a senior police officer have also been included.

Incidents of Terrorism in KP Province

The data on terrorism incidents obtained from the police department of KP* is given in Table 1 below. As evident from Table 1, the number of terrorist cases registered in KP has significantly decreased in the year 2010. There were 727 cases registered in the province in 2009, and 252 in 2010, i.e. a decrease of more than 60% from 2009. The total number of fatalities reported in 2009 were 1,020, which included the highest number of civilians 742, 107 personnel of army troops, 22 personnel of Frontier Constabulary (FC) and 149 policemen. In 2010 the number of fatalities has decreased considerably. The total number of persons killed was 524, which included 412 civilians, 37 army troops, 12 personnel of FC and 63 policemen. It means that the civilian population is the highest victim of terrorism incidents.

Table 1: Details of Terrorist Activities: Explosions, Missile Attacks, Firing, Suicidal Attacks and Blast at CDs/Barber Shops etc
(For the years 2009 and 2010)

Years	No. of Cases Registered	Person Killed					Person Injured				
		Police	FC*	Army	Civilian	**Total**	Police	FC	Army	Civilian	**Total**
2009	727	149	22	107	742	**1020**	360	70	236	2244	**2910**
2010	252	63	12	37	412	**524**	197	18	105	1047	**1367**
Total	**979**	**212**	**34**	**144**	**1154**	**1544**	**557**	**88**	**341**	**3291**	**4277**

Source: SP/Research, Central Police Office, Khyber Pakhtunkhwa, Peshawar, Pakistan
Frontier Constabulary

*Khyber Pakhtunkhwa previously known as the North-West Frontier Province and various other names, is one of the four provinces of Pakistan, located in the north-west of the country. It borders Afghanistan to the north-west, Gilgit-Baltistan to the north-east, Pakistan administered Kashmir to the east, the Federally Administered Tribal Areas (FATA) to the west and south and Punjab and the Islamabad Capital Territory to the south-east. The majority inhabitants are Pashthuns. For further detail see also,
http://www.khyberpakhtunkhwa.gov.pk/

There is also a considerable decrease in the number of injured person in 2010. A total of 2,910 were injured in 2009 but fell down to 1,367 in 2010. The total number of people reported injured in 2009 was 2,910, which included the highest number of civilians as 2,244 with 236 army officers, 70 personnel of FC and 360 policemen. Whereas, in 2010 the total number of casualties reported was 1,367, which included 1,047 civilians, 105 army officers, 18 personnel of FC and 197 policemen. Again, the civilians remained the most affected by terrorism incidents.

Whilst this decrease in cases and fatalities is encouraging in the KP region, such statistics provides a glimpse into the dangerousness of the context in which frontline police are required to carry out and manage terrorism investigations.

Results: Findings and Discussion

The findings from the research interviews with police officials into several investigative constraints faced by frontline police in the KP province are presented and discussed in summarized form below.

1. Constraints in Crime Scene Preservation

Crime scene investigation provides the permanent records of the crime and the material that are collected at the scene. It plays a pivotal role in ensuring a successful case file for prosecution. Therefore, protecting and preserving it from contamination facilitates successful prosecution which is dependent upon the physical state of the evidence collected at the scene. The protection of the scene begins with the arrival of the first officer of the law enforcement agencies at the scene and ends when the scene is released from police custody. Careful and thorough investigation is the key to ensure that potential physical evidence is not tainted or destroyed or potential evidences overlooked.

However in Pakistan, when a suicide or other attack occurs, the preservation of crime scene becomes a challenge for the LEAs. All of a sudden, a mad rush of mob towards the crime scene is a usual picture. One of the interviewees said, that "*the first problem we encounter in terrorism incidents, e.g. bomb blast, is the mob of people*"[1]. Police are often confronted with public anger, non-cooperation and disorderliness. This public confrontation possesses serious problems for police in the preservation of crime scene. He further pointed out that "*the rush of the people at the crime scene results in the contamination of crime scene and trampling of important evidence*". Moreover, as mentioned by Fasihuddin (2010), the media race for early coverage and too many cameras also hamper the job of LEAs to preserve the scene. Another problem that hinders the preservation of crime scene are the primitive methods to preserve the scene. These factors further create a mess for the police when it comes to knowledge that the police don't have Standard Operating Procedures (SOPs)

for crime scene preservation. As per Police Rules 1934 (Rule No. 29.60, Chapter 29. Volume No. 3),[2] an investigating officer should have an Investigating Bag with all necessary gadgets, equipments for early preservation of small, trace evidence and collection of items from the scene of crime. One of the interviewees said that "*hardly, I have seen an officer with a bag. It is not officially provided to them"*[3]. This non-professional attitude speaks volumes of the police incompetence to preserve the scene of crime.

2. Constraints of Witness and Recovery

More significant in investigation management of terrorism cases is the problem of witnesses and recovery. Unfortunately, in our country we don't have any effective programme for witness protection and security. Fear and threat to life makes the witness reluctant to come forward. At times, due to withdrawal from the statements, and due to fear of enmity or retaliation from criminal gangs, the witnesses don't take active part in investigation processes. Often the contradictory ocular statements is another constraint to the benefit of the accused. One interviewee pointed out that *"most of the cases acquitted in the court are due to the witnesses' statements, their contradictions and withdrawal"*[4]. In the areas of military operations, the terrorists are generally apprehended by the military and para-military forces who, at a later stage, are handed over to the police for criminal proceedings against them. The military doesn't take any responsibility for producing evidence in the court and hence the case is susceptible to failure. The fear or indifference on part of the general public leaves no other option except for the police witnesses. "*Unfortunately, the statements given by the accused in front of the police officer under Section 161 of the Criminal Procedure Code 1898, are not admissible in the court of law, and the judiciary gives little importance to police witnesses if they are the sole witnesses in a case."*[5] The recoveries so made are thus left only to police attestation.

Table 2. Details of Recoveries of Terrorist Explosives and other Weapons

ITEM	2007	2008	2009	2010	21 - 07 - 2011 (11 - 07 - 2011)
No. of Cases Registered	75	94	116	72.00	66.000
Explosive Material (in Kgs)	122	52366	5898	440.70	958.662
Explosive Jackets	20	20	20	5.00	4.000
Hand grenades/ Dynamites, Detonators & Anti Tank Mines	190	481	14301	66999.00	26893.000
Rocket Launchers, Bombs, Missiles & Mortar Missile Shells	220	93	656	261.00	25.000

ITEM	2007	2008	2009	2010	21 - 07 - 2011 (11 - 07 - 2011)
Prima Chord (Explosive Wire)	N/A	N/A	10857	2871.00 (2 Bundle)	77.000 (15 Bundle)
Safety Fuse in Meter	N/A	N/A	26036	5707.00	2860.000

Source: SP/Research, Central Police Office, Khyber Pakhtunkhwa, Peshawar, Pakistan

Table 2 shows the recovery of explosives, weapons and other items like suicide jackets by the KP Police in 2007—2010, but again, most of these recoveries don't' add to the police performance in terms of arrest or conviction of the suspects. Mostly, these recoveries are made without any carrying persons, like from a suspected place or house in a deserted/un-frequented area or from disbanded or left vehicle or any other suspicious consignment. This kind of recoveries are not trusted by the general public as police in this country are usually blamed for fake-recoveries jut to show and inflate their un-founded performance. In reality, such recoveries have never deterred the terrorists from carrying out their nefarious activities, and also we have hardly seen any conviction on the basis of these large-scale impressive recoveries as in most cases neither the culprits are arrested nor the memos of recoveries are prepared, signed and verified by the police with the proper legal procedures, hence easy acquittal and no conviction.[6] Moreover, the police in KP claims the dismantling and disposal of bombs and other explosive materials by the Bomb Disposal Squad (BDS), but again, such good work doesn't lead to any conviction or arrest as, in such disposals, criminal cases are not registered per policy, hence no investigation, no tracing and no prosecution. The KP Police claim 317 disposal in the first half of the year 2011.

3. Multiplicity of Agencies

It is also a major constraint on part of the security forces to determine the area of jurisdiction. In many incidents of terrorism, the initial interrogation is carried out by the Army or Frontier Corps. Then, at the time of the registration of cases, the police are not given access to the original or early pieces of evidence. Mostly, the military, the police and other security agencies are jointly involved in such operations. It becomes difficult to determine that which particular agency would conduct investigation or take the responsibility for possession or enjoy the powers of decision-making on the spot. Army has its own procedure, different from that of the police and paramilitary forces. So, besides the police, there are many more players, as mentioned by Ghani (2010), involved in investigation of terrorism cases, like Levies, Army, Khasadar,

Frontier Corps, and Frontier Constabulary. Every LEAs has its own way on conducting investigation and interrogation. Unfortunately, there has been no coordination amongst the LEAs, which is hampering the job of the police in registration of cases, hence, faulty investigation. The reports of the Joint Investigation Teams (JITs) are also legally debated and don't form part and parcel of the case file for prosecution (Fasihuddin, 2010).

4. Constraints of Forensic Sciences Tools of Investigation

Forensic Science can be defined as criminalist science. Such facilities as DNA tests, finger prints, eye matching, sampling examination in the laboratories, keeping record of national database programme for cross examination of the samples, etc are operational in the investigation processes and quite frequently available in the modern world, but very rarely and poorly seen in Pakistan. Unfortunately, in Pakistan, there is no state of the art forensic science laboratory. The Forensic Science Laboratories (FSL) were not reformed and modernized in the wake of creating new and specialized units in the police under the new Police Order 2002. Furthermore, there is a dearth of equipments and trained staff for the operation of Forensic Science Laboratories. The situation in KP is not different from the rest of the country. The FSL in KP were not modernized and reformed. The FSL infrastructure in KP is not well-furnished. There is a lack of trained staff and modern equipments for forensic science testing. The police in KP do not have ample resources for detective instruments and up gradation and modernization of their Forensic Science Laboratory.[7]

The FSL in KP was established in 1976. In 1978 the total staff of the FSL was 78. It included ministerial, technical and other staff. The available staff examined a total of 2500 cases in 1978. Today, after thirty-four years of its establishment, the FSL has a total of 82 staff members. The available staff examined 52,721 cases in 2010. This means that 643 cases were being examined by each examiner in 2010 and a total of 144 each day. The total cases include all kinds of offenses like narcotics, arms, explosives, rape, vehicle tampering, and so on. It is important to mention that the DNA test, which is mostly carried out in terrorism cases, is out of the boundaries of FSL, KP. The FSL in KP does not examine the DNA tests. For the DNA test, the samples are sent to Islamabad, which takes at least seven (7) days to complete. Further, the cost of DNA test is also very high. At average, a single DNA test costs Rupees (Rs). 30,000 ($ 345 USD). The total budget of FSL for purchase of chemicals was increased from Rs. 500,000 ($5,747 USD) to 1,000,000 ($11,494 USD) in 2010. This is a very meager amount for the purchase of costly chemicals, the price of which is always on the increase. It shows that FSL was given an allocation of Rs. 19 ($ 0.218 USD) for every single examination at average in 2010.[8]

5. Constraints of Intelligence-Based Investigations

In the western world intelligence is the backbone of this new concept of the Intelligence-Led-Policing (ILD). Much literature is available on the subject now. Unfortunately, the LEAs in Pakistan have not embraced this concept yet. Our intelligence system is mainly in the hands of army. The Special Branch (SB) of the police department is relatively poorly developed and weak, whereas the units of the Central Intelligence Agency (CIA) and the Criminal Intelligence Department (CID) have become defunct after the new police reforms in 2002. Police generally apply the routine techniques of investigation, even for the deadliest cases of terrorist or suicide attacks, where in the absence of CCTV or eyewitnesses, or huge destruction, the evidence is badly destroyed and trampled. The investigating officers (IOs) are not properly trained. These untrained IOs often avoid conducting investigation of terrorism cases. The major reason for avoiding responsibility in this respect is the non availability of resources, and lack of professionalism. Moreover, the police officials fear the potential consequences of dealing with such cases.[9]

Therefore, they fail to devise a plan to bring the criminals to books and do a rational profiling of the potential terrorists, or identify groups at risk in a locality. The Khyber Pakhtunkhwa police also tried to formulate an extensive profiling system, but could not materialize it into a sound computerized system. This profiling system was basically designed for the more than four thousands terrorist/suspects who were arrested during the military operation in Swat in 2008-09. The most interesting part of this profiling system is that it was all based on the interrogation report of the Joint-Interrogation Team, an arrangement of all local civil and military agencies and police. The eight pages comprehensive interrogation report proforma is full of indicators, personal, familial, social, religious and organizational of a terrorist suspect. In addition to finger prints, photo, brief life history, and opinions of the investigator to classify the accused as black, grey or white, there are 120 indicators or questions about the various aspects of an accused's personal or family and organizational attachment, including the unnecessary question and information about a suspects' maternal and paternal grandfather, uncles, brothers, sisters, their children and their mobile phone contact! An officer told on the condition of anonymity that "*this procedure of interrogation and investigation was deliberately made lengthy, time-consuming and full of unnecessary items so as to gain time and avoid responsibility by the senior police officers and investigators"*. To be honest, indeed, nothing came out of

this non-professional and non-institutional attitude. The police leadership must have worked for a state of the art forensic sciences laboratories in the last decade of war on terror, for which they could easily re-allocate their funds or have approached different UN or donor agencies.

However, in the routine police work, the role of the intelligence units in gathering information, making criminal profile of a terrorist and report on any potential threats by local police wings like the Central Intelligence Agency (CIA) and Criminal Intelligence Department (CID) is very important, but no meaningful steps have been taken to make these wings functional and operational for a productive and result-oriented intelligence system. As suggested by Fasihuddin (2010), it needs an academic and intellectual input from senior intelligence analysts and an immediate revitalization of CIA at the district level and the CID under the Investigation wing of the Provincial Police Department with the same role as given in the Police Rules, 1934 (Rules 21. 35 for CIA, and Rules 21.25 for CID). New amendments can be made to it in accordance with the circumstances and requirements. This will undoubtedly overcome the intelligence gap of the investigation management of the terrorist cases.[10]

6. Constraints of Cost of Investigation

Another daunting problem that slows down the investigation management of terrorism cases is the cost of investigation. The problem in the cost of investigation that confronts the police is lack of resources with the investigation team for carrying out the smooth processes of investigation. The cost of investigation in the KP for the year 2007-08 was 25 million rupees (about $ 280,898 USD) and in 2008-09 it was 19.85 million rupees (about $ 223,033 USD). For the year 2010 it was 20 million rupees ($ 229,885 USD)[11]. As mentioned in Table I the total registered crimes for the year 2010 were 136,665. By these figures we get less than Rs. 150 ($ 1.7 USD) for each case in Khyber Pakhtunkhwa. This poor financial back-up of investigation speaks for itself. The cost of investigation includes support to the investigator and the accused in daily traveling, communications and food allowance, etc. But this is the simple assessment of all cases are available funds. The real thing is that the cost of investigation is distributed according to the Standing Order No. 3/2007 of the Provincial Police Officer which shows different rates for cost of investigation in different crimes.

In the opinion of the writer as being a senior police officer, the criteria for the cost of investigation should be re-defined and the maximum allocation should be made for cultivating informants. The phenomenon of breeding trust - worthy informers in targeted organizations and criminal gangs is of paramount

importance to local police. Unfortunately, the police in Pakistan don't receive any special funds for this purpose. The investigators often make such provisions from their pocket money (to some ill-gotten!) or oblige the informer with other local services like a school boy admission, easy gas or electricity connection, etc. The only available Secret Service (SS) Funds are not generally distributed by the police headquarters to the lower offices. It is not equitably distributed and even the exact amount of this money is generally not known to the outside of the department. Actually, almost the total police budget is spent (88%) on establishment like salaries and allowances and only 12% is left to qualitative expenditures which is a very meager amount and nothing can be reasonably allocated to information-buying. The official record of KP Police shows an allocation of SS Funds as 5.500 million rupees (about $ 61,797.75 USD) for 2007-08 Financial Year and 3.008 million rupees (about $ 33,797.75 USD) for 2008-09, for the whole KP Province. Even if this amount is utilized wisely and carefully, it can bring a good deal of credible information.

Though, it is an open secret that most of our local police stations still heavily depend on local informers, information by notables and tips by media-men and local intelligence agencies, yet no one takes the risk of giving information on any terrorist or militant organization. The reason is very clear. People are afraid of the retaliation and repercussion after it is known that from whom this information was purchased. “Don't you see that every now and then, a man is beheaded in the tribal areas by Taliban and his dead body is thrown in a field or market with a letter that such is fate of a spy of America”, said a police officer.[12] This is why people avoid to be informers for the police in cases to terrorism offences as no one knows when the identity of the informer is disclosed and his days start numbering.

7. Constraints of Crime-Terror Continuum Identification

Makarenko (2003) has developed a hypothesis of 'crime-terror continuum' (CTC), which explains the relationship of the 'crime-terror nexus' in the contemporary security environment. It is called a '*continuum'* because it may be used to trace past, current and the potential future evolution of organized crime and/or terrorism. It also alludes to the fact that a single group can slide up and down the scale depending on the environment in which it operates. The most instable and threatening point along the CTC is the fulcrum point, where criminal and political motivations simultaneously converge and are displayed in the actions of a single group (Makarenko, 2003). Though the 'Convergence Thesis' is a good linear transformation hypothesis of political organizations turning into criminal / terrorist groups, the difficulties of identifying such

groups and predicting the exact time of such transformation and its precipitating factors are always a challenge to the security people who are required to be a step ahead of such triggering processes.

The terrorists live in symbiosis and in a state of interdependent equilibrium with other organized crime gangs. They rely on each other's capabilities, technical know-how, experiences, training, motivation, contacts and resources. The support of drug mafia and poppy-growers to the ruling Taliban in Afghanistan before 9/11 is still resonating in the western academic and official circles. Same is the case in Pakistan where people involved in white-collar crimes, car-snatching, serial killing, vehicle theft, drugs pushing, kidnapping, chronic non-payment of taxes, arms dealing, smuggling of non-custom paid vehicles, etc have identified themselves with the invisible Taliban groups in various parts of tribal and settled areas. Similarly, certain hardened criminals of settled districts have joined various Taliban groups for the purpose of shelter, economic benefit and group synergism. Some strongly religiously intoxicated groups of Taliban don't approve of these notorious gangsters and criminals but due to the ongoing war on terror they have welcomed them out of exigencies and as a matter of convenience.[13]

8. Constraints in Prosecution, Case Building and Conviction

Prosecutors are covered under section 492 of the Criminal Procedure Code (CrPC) which provides that the provincial government may appoint "generally or in any case, or for any specified class of cases, in any local area, one or more officers to be called Public Prosecutors".[14] Until recently, the prosecution services in all the provinces were under the Home Department and were administered by the police.[15] There was a separate prosecution branch of the police consisting of law graduates in the ranks of Deputy Superintendents of Police, Inspectors and Sub-Inspectors. This was considered, however, to be a major reason for poor prosecution and delay in the resolution of court cases. During the 1980s, a first attempt was made to transfer administrative control of prosecution powers from the police to law departments.[16] The ongoing vacillation between the Home Departments and the Law Departments on this question continued until prosecution services were permanently placed under the administrative control of the Law Departments with the promulgation of the Police Order, 2002. At present, all the provinces have laws for separate prosecution services and the respective provincial prosecution services are at nascent stages of development.[17] The prosecutorial services in KP were introduced through the North-West Frontier Province Prosecution Services (Constitution, Function and Powers) Act, 2005.

The problems of prosecution and case building are manifold. The prosecutor office is severely understaffed. Due to which there is large number of previously pending cases. It is evident that the distribution of cases is not only skewed but also creates problems of corruption, injustice and delay in provision of justice. Justice delayed is justice denied. The appointment of prosecutor is also a grey area; politician, bureaucrats and big lawyers heavily influence the recruitment process (Mirza, 2010). Furthermore, there is no defined infrastructure of prosecution in KP. There is no coordination between police and prosecution which results in weak prosecution that leads to the release of terror suspects. Moreover, the case building process is not conducted on modern lines. The poor record maintained by the Investigation Officer (IOs) and the ineffective case file record system and lack of sanctity of police record further adds complexities to the investigation of terrorism cases.

Generally conviction rates by the prosecution have been abysmally low, but it must be emphasized here that the prosecutor places before the court all the evidence in his or her possession, whether in favor of or against the accused. According to newspaper reports, the overall conviction rate in terrorist cases stood at 5% (Amin, 2011). However, the official conviction rate, as provided by the Central Police Office, KP, is 14%. This is a clear contradiction. When asked, the officials of Central Police Office pointed out the usage of different formulae which render different conviction rate (a statistical discrepancy)!

In an official briefing on internal security situation, a military officer reportedly said that 695 suspected militants out of the 1443 who were detained had been bailed out, mostly by appellate courts, while 48 others were acquitted by anti-terrorism courts. The same meeting noted that the only conviction delivered so far by an anti-terrorism court was when a militant, Noorani Gull, was handed down a sentence of 120 years in jail (Amin, 2011). The disconnect between the police and the prosecution is a depressing and detrimental aspect of the overall investigation management of crimes, especially of terrorism incidents. Despite the new law of prosecution in 2005 and its separation from the police, the prosecution is not fully developed in terms of human and physical resources.

9. Constraints of Area of Jurisdiction and Territorial Responsibility

The trickiest aspect of the investigation is the territorial responsibility of the LEAs in Pakistan. Most of the terrorists' safe-havens and outfits are in the Federally Administered Tribal Area (FATA) where the police have no jurisdiction of their own. In case of an incident, if a terrorist is suspected to have his origin in the tribal area, it is next to impossible for the police to enter into the tribal belt for any arrest or collection of evidence. The extremely damaged civil administration in the FATA due to the ongoing serious military operations and

US Drones Attacks, and due to the grave in-coordination amongst other law-enforcing agencies in the tribal belt, the police have no access to any group or gang for the purpose of criminal intelligence and investigation. This difficulty of the area of jurisdiction and territorial responsibility gives rise to serious impediments for police investigation of crimes in general and of terrorism in particular. Except Kurram Agency, all other tribal agencies are contagious with the settled/urban districts. The borders of the settled districts and tribal belt are to be guarded, protected and patrolled by the Frontier Constabulary (FC), a force of more than 20, 000, raised mainly from the known tribes and administered by the officers of the Police Service of Pakistan (PSP). FC was established in 1913 by the then British colonial rulers in un-divided India. However, most of this force is now engaged in assisting the local police in the urban areas like Karachi, Islamabad, Peshawar, etc. The usual and designated duties of the FC faded out with the passage of time, so the internal borders are now poorly policed and controlled.

10. Constraints of Human Resources in Investigation Wing of Police

After the new police law, the Police Order 2002, the police in Pakistan have become badly compartmentalized and divided into separate so-called specialized units. However, as stated earlier, the policemen prefer to opt for prevention than to stay in investigation for cumbersome processes, recoveries and case-building. They generally use influence of various kinds in order to run away from the under-resourced investigation wing. Moreover, the division of police into prevention and investigation is not fairly equal or substantially proportional. For example, in the Province of KP, the total police strength is 76,582 which is divided into a slot of preventive officials as 72,283 and the investigators as 4298. It means that 94% staff is in prevention and 6% makes the investigation wing. On the other hand, the total registered crimes in the Province are 136,665 which include all kinds of cases against property and person and for an effective investigation we have 31 cases for one investigator. It is to be mentioned that under the law, Section 172 Criminal Procedure Code 1898, an investigation officer is required to submit his progress in the form of a Case Diary, called *Zimni* on daily basis and if he omits the investigation of a case for quite sometime, he has to give reasons for his delay and time break in the investigation processes. One can imagine how badly these investigators are overburdened with the routine work of investigation. Moreover, we have no specialized police for investigating the cases of terrorism like suicide bombing and blast of explosive-ladden vehicles, and the same are investigated by the regular and lethargic investigation staff. Interestingly, all the staff of the investigation wing are not authorized to conduct investigations. Only Assistant Sub-Inspector (ASI) and above officers are legally authorized. Lower-staff are generally an auxiliary and helping hands.[18]

11. Constraints in Investigation of Suicide Bombing

Suicide bombing is the worst of all terrorist attacks. Even 9/11 attacks were suicide attacks. Police never saw such deadly weapon with potentially of immensely large devastation and targeted killings. Similarly, never suicide bombing was used by any terrorist organization after the recent US-Afghan war on terror. Moreover, the religious motivation behind armed resistance remained a clear sign in all monotheistic religions, but the suicide bombing phenomenon is only seen in the radicalized Muslim militants. The number of suicide attacks in the overall terrorist incidents may be smaller but in terms of physical and psychological damage, its impact is far than anything. The investigation of the suicide bombing is the most difficult as the police deterrence is of no effect to the perpetrator. In addition, little is left to investigate as only a DNA testing of the suicide killer is of little importance as we don't' have a national data-base for such testing and the tribal ethnicity or family background speak very little of the overall motivational and radicalization processes and training of the bomber, as police have no jurisdiction in the remote tribal areas or Afghanistan. It is generally said that suicide bombings are made as a response to the Pak-Army military operations and the US-Drone attacks in the tribal areas, however, mostly police are targeted in the urban areas who have nothing to do with the military operations or Drone-Attacks in the tribal belt, so it makes us confused about the whole phenomenon of the suicide bombing.

Moreover, the would-be suicide bombers are rarely convicted due to other investigation constraints as mentioned in this paper. At times, media make frontline stories of the arrest of a would-be suicide bomber, e.g; of a 9-year girl who was purchased by someone for a suicide attack (Khan, Tuesday, June 21, 2011).[19] However, due to retraction from statement, the case was spoiled and the whole story became suspicious (Khan, Wednesday, June 22, 2011).[20] At times, the issue of suicide bombing becomes political when Pakistan blames Afghanistan a safe-place for indoctrination, and on the other hand reports from Afghanistan claim that suicide bombers are usually prepared by and sold to the Haqqani Group of Taliban for 40-80 lac rupees.[21] However, such statements need to be verified from the case files and other authentic resources. All these factors make the investigation of suicide bombing the difficult aspect of police investigation.

12. Legal Constraints in Investigation of Terrorism Cases

After the arrest of an accused, the local police are bound to produce the accused before a Magistrate of competent authority in 24 hours. This is a legal obligation under Section 61 of the Criminal Procedure Code, 1898. The police

then demands custody of the accused for investigation, recovery, collection and recording of evidence and confession. The usual limit of police custody for other crimes is up to 14 days, which, however, are not granted in full or in parts by the courts. The courts usually grant the police 2-3 days custody at a stretch and rarely extends it if the police fail to argue strongly enough for grant of more custody. On the contrary, the terrorist/suspects arrested under the Anti-Terrorism Act (ATA) of 1997 are granted more days of police custody but again not exceeding seven (7) days. According to the Anti-terrorism (Amendment) Ordinance VI of 2002), dated 31 Jan, 2002, the person detained for investigation may be kept in police custody (Remand, under Section 21E) for a maximum period of 15 days, which is extendable to 30 days in case of further request by the police but to the satisfaction of the court. Under Section 11EEE (Amendment Ordinance (CXXV of 2002), dated 15th November, 2002), the government can arrest and detain a suspect for certain period but not exceeding a total period of 12 months.

Some of the amendments were done in the ATA, 1997 through an ordinance, but due to non-issuance of the same again or ratifying the same by the parliament, the amendments lapsed and the ATA, 1997 remains the same as unchanged.

However, the debate goes on in Pakistan that the anti-terror law needs serious amendments like giving free hand to the police for siege and search, arrest without warrant, an unlimited or quite long authority of police custody, police recorded statements be admissible in the court of law as evidence, and making room for production of military officials as witnesses in the competent court. Justice Maqbool Baqar of Sindh High Court, while presenting at a paper at a seminar on criminal justice dispensation, prosecution and investigation of All Pakistan Judicial Academies Summit, suggested that "Anti-Terrorism Act should be amended to limit its application to purely terrorist and sectarian offences, and other heinous offences cases should be assigned to different ATCs (Khurshid, 2011)." According to a press report (Yasin, 2011), the Prime Minister while chairing the Defence Committee on May 25th, 2011 decided to authorize the security defence and law-enforcement agencies (LEAs) to use all means necessary to eliminate terrorists and militants.[22] Such political statements, are, however, need to be substantiated by proper orders or changes in laws. However, such enormous police powers in other countries have also been seriously criticized by human rights activists and civil society. No doubt, power corrupts and absolute power corrupt absolutely. At times, people forget and ignore the severity of the stringent laws in countering terrorism at the initial phases of responding to the serious blasts and utter destruction, but soon after

the wave of terror subsides and the injuries recede into background, people start feeling annoyed and violated on these strict implementation of unusual laws. Literature on this subject of violation of public rights and privacy and anti-terror laws is becoming more and more. This is one of the major constraints in dealing with terrorism cases as, from a police perspective, the investigator must be covered legally for his/her job in tracing and establishing a case of terrorist incident.

13. Constraints of Shifting Responsibilities

Another serious constraint is the mutual bizarre shape of accusations of the wings of criminal justice system in Pakistan. Everyone wants to pass on the bucket to the other as to avoid public indignation for not bringing terrorists to the court of law and convict them properly. A series of statements in the press are seen from different wings to malign the other for shortcomings, laxity and incompetence, even being accomplice. It is in this backdrop of mutual accusations that the higher judiciary took notice and a few meetings have been held now to thrash out the differences amongst the various parts of the criminal justice system.

For any prosecution department to be successful and submit cases with best evidence before the courts, good relationship with the police is crucial. If the prosecution department and the police department are at loggerheads, or are working without any coordination, then the cases churned out will be like the cases in Pakistan that lack sufficient evidence and thus result in the acquittal of dangerous terrorists who had been arrested with great difficulties (Mirza, 2010). The press reports in this context are not without interest for the reader. Two different press coverages are hereby reproduced which throw ample light on the intrinsic and complex constraints of investigation management of terrorism cases in Pakistan

A meeting of Criminal Justice Committee was held under the chairmanship of Dr. Faqir Hussain, the Registrar, Supreme Court of Pakistan. The meeting discussed the issues related to non-submission of *challan* (Final Report), litigation, non-production of under-trail prisoners and other issues ancillary to administration of criminal justice system. The meeting also considered various issues and problems which cause delay in completion of investigation and submission of *challan* before the court of law, including lack of Forensic Science Laboratories and modern techniques in crime detection. The Provincial Prosecutors Generals informed that there is a shortage of prosecutors which causes delays in finalization of cases. On the other hand, investigation officers are lacking required qualifications and skills; therefore, acquittal rate is high which is affecting the image of the justice sector institutions in general and judiciary in particular (*The News*, May 16, 2011).

The overall conviction rate in terrorist case stood at five percent. The situation became so alarming that officials from KP and senior military officials held a meeting to find out ways to overcome the problem. The government officials cite several cases where, they believe, the courts refused to accept the prosecution evidence and freed dangerous terrorists. Neither the judiciary nor the executive is satisfied with the existing anti-terrorism laws and the performance of anti-terrorism courts. Prime Minister Yousf Raza Gilani recently admitted in the National Assembly that anti-terrorism laws needed to be tightened, as he was concerned that terrorists apprehended by the LEAs had been bailed out and were again indulging in terrorist activities (Amin, 2011).

In further response from the Chief Justice of Pakistan, Justice Iftikhar Muhammad Choudhry, while speaking to a conference of All Pakistan Judicial Academies Summit in Karachi on June 26, 2011, he remarked, "the investigation agencies and police play a vital role in the dispensation of justice, particularly in the criminal matters, and any lacunae on the part of investigation agency badly damages the prosecution case so that there is dire need to improve the quality of investigation by educating the investigators with the current laws and equipping them with necessary paraphernalia". The Honourable Chief Justice of Pakistan while lamenting the ineffective role of the new police law, the Police Order 2002, the lack of coordination amongst the various stakeholders of the criminal justice system at the lower level and the resultantly low conviction rate, said that "greater responsibility is put on the shoulders of those who have to participate in the process of administration of justice, and any error or flaw and laxity make the judge accountable in this world and the world hereafter" (Khurshid, 2011).

14. Constraints in Investigating Financing Terrorism

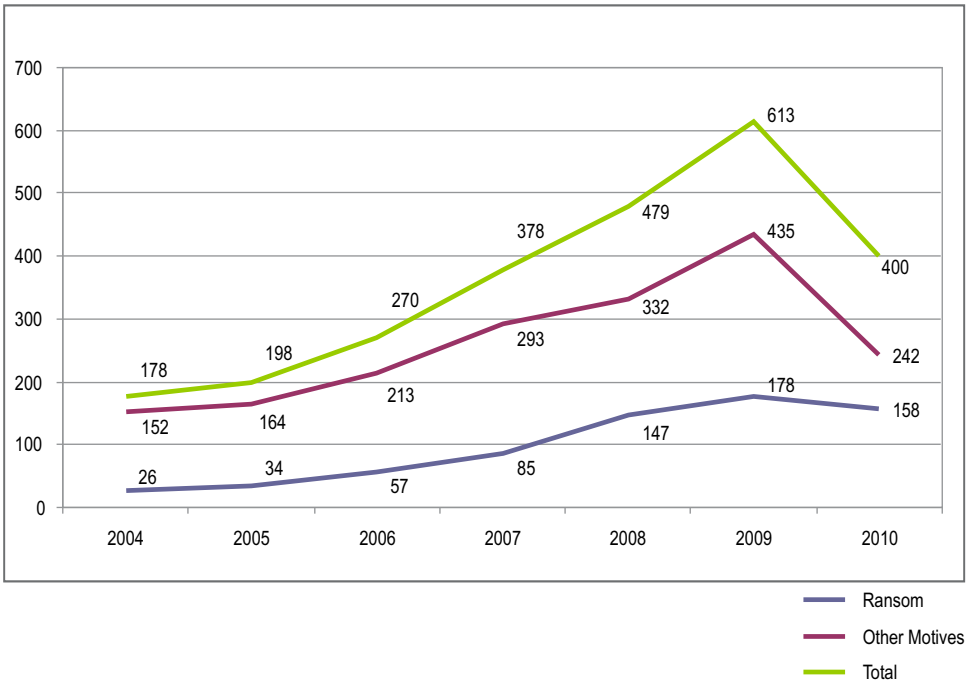
"Terrorist financing is very different today. Five years ago, we had large movement of funds which went through the international financial system. Now we are just talking about four friends who raise £1,000 to stage an attack. The unit cost of terrorist financing has crashed to the floor. They [terrorists] don't need another 9/11. They can do a small thing and create the same hysteria (Oxley, March 8, 2006)." This analysis is also true for Pakistan where tracing the complex cascade of financing terrorism doesn't fall in the jurisdiction of the local police and the terrorists don't need big attacks as they do larger attacks occasionally and small-scale attacks regularly.

There are five kinds of financing a terrorist organization; one is the charity, alms and donations to the local Taliban groups or banned organizations by individuals, families or small trade groups, especially the transporters. But this is generally done out of religious commitment and Islamic feelings for the local

groups. This kind of financing support can't be traced as it is not generally made through cheques, banks-transfer or on receipts. Legally, charity and donations to someone is not a crime. The second kind of financial support is the generation of resources through illegal activities by terrorist groups like poppy-cultivation, drugs and arms smuggling and kidnapping of important personalities for ransom (Khan & Sajid, 2010). This aspect is too much trumpeted by the western writers and media as a major financial support for local and Afghan Taliban, but in reality little empirical research can substantiate and validate this observation. The increase in kidnapping in KP during serious Taliban insurgency in 2007-2009 as shown in the following graph (Figure I) is generally attributed to this observation. But, on the contrary, the police investigation files can't establish this observation. The opposite view is that since police were badly attacked and got engaged in the fight against terrorism, so they had little time for routine policing and their attention got diverted to the more serious and active fight than normal investigation and prevention measures in local community.

The third kind of financing terrorism is the generation of resources as a fee for their services to local community like solving their disputes or recovery of their outstanding loans. This is one of the widely known methods of resource generation by the local Taliban as they believe in speedy justice and quick dispensation, and people are tired of lengthy litigations for years in the civil courts particularly. This is also one of the major reasons of the Taliban's initial popularity in an area. This service delivery of Taliban can be compared to the mediation services of the developed societies like Singapore and Malaysia. However, again police can't investigate such cases as on the one hand police have no jurisdiction in most of the civil disputes, neither they can take cognizance of such matters nor people report their personal civil matters to them, and on the other hand local Taliban solve and decide such issues in the nearby tribal areas where, as earlier stated, police have no jurisdiction.

Figure I: Kidnapping in Khyber Pakhtunkhwa (2004-2010)



Source: Office of the Superintendent Police (Research),Central Police Office, Khyber Pakhtunkhwa, Pakistan.

The fourth kind of financing terrorism is generating resources through looting and plundering of natural resources. For example, in Swat during 2006-08, i.e; during the high scale insurgency of Taliban, costly forests were destroyed, trees were cut and mines of precious stones were looted. Despite their outrageous looting of natural resources, no official statistics are available on the actual cost to the public property, which by no means will be less than millions of dollars. In his article, 'The Political Economy of Taliban Terror in Swat', Tom Burghardt (2009) quoted an Abu Dhabi-based newspaper, The National, April 3, 2009, that *militants are funding a campaign of violence with profits made from the illegal mining of emeralds and felling of timber in the volatile valley of Swat in northern Pakistan* (Burghardt, 2009).[23] He added that after looting the collective wealth of Swat's citizens, the gems "are then smuggled to Jaipur, India, before being transported to Bangkok, Switzerland and Israel (Burghardt, 2009)." It implies that the threads of financing terror are spread throughout the world.

The last kind of financing terrorism is the major portion of the economy of terrorism. The State Bank of Pakistan sends bundles of details of Suspicious Transactions (ST) observed in different country banks to the Federal Investigation Agency (FIA) for discreet probe as from where and why such huge transactions have been made in such accounts in the local banks. The banks normally do not cooperate with the FIA as they need more and more deposits, and are least bothered to trace the origin and reasons for such transactions. Unfortunately, the Anti-Money Laundering Act was enacted in 2010 which is a recent law and under the law the FIA can take action only if the suspicious transaction is shown as "the proceeds of crime" (Naseer, 2010). The FIA has the jurisdiction on such matters, but unfortunately, the staff of the FIA has no training, resources, and at times, courage to investigate these matters. These suspicious transactions are generally made in fake names and the accounts are usually closed after the transactions are made. We have yet to see registration of such criminal cases under this law and conviction made. It is too early to predict such things. The FIA is secretive and reserved to share the information of these suspicious transactions with anyone outside the Agency.

Table 3 : Details of Suspicious Transactions in Pakistan - From 2009 to 30th May, 2011

Zone	2009	2010	2011	Total	% age
Quetta	4	5	0	**9**	6%
Islamabad	2	5	2	**9**	6%
KPK	5	20	7	**32**	20%
Punjab	7	22	10	**39**	24%
Karachi	21	31	22	**74**	45%
Total	**39**	**83**	**41**	**163**	100%

Source: Economic Crime Wing, FIA, FIA-Headquarters, Islamabad, Pakistan.

However, the writer got the data of Suspicious Transaction from the FIA Headquarter, Economic Crime wing, Islamabad, which were received to the Wing from the State Bank of Pakistan. Table IV shows the total number of enquiries up-till May 30th 2011. It is pertinent to mention that the major number of enquiries pertain to Karachi zone followed by the Province of Punjab. The number of enquiries has considerably increased in 2010, which is probably the result of the new anti-money-laundering law of 2010.[24] However, little is to the credit of the FIA for turning these enquiries into criminal cases and conviction. It is after a successful investigation that we may be able to link these suspicious transactions of financing the terrorist groups. It is also not clear from this wholesome data that how much money was involved, however, the writer as en-ex Director of FIA, KP zone personally knows that some of these enquiries involve multi-millions of dollars as suspicious transactions.

Conclusion

Investigation of terrorism remained a missing link in counter terrorism studies and policies. Investigation is the prime activity for the strategic move in the hands of the law-enforcement agencies. Hesitation or non-availability of the witnesses, poor prosecution and in-effective case building, and lack of capacity and knowledge to investigate terrorism cases are but a few of the major constraints in terrorism cases. The policy makers need to give equal importance to the investigation and prosecution of terrorism. Effective and result-oriented investigation can discourage further acts of terrorism. It is extremely rare to find out a good empirical research study on investigation of terrorism in Pakistan. This research is the first of its kind in Pakistan. The research for this paper adopted an interview method to find out about the multiplicity of constraints facing frontline police investigating terrorism cases in Pakistan. There is a need for more in-depth and empirical studies in this area.

In the final analysis, the author agrees with the assessment quoted below by Duma (2009) that countering terrorism is both a short-term and long-term problem in which frontline police play their part.

> *"There are much more effective ways to respond to terrorism, and even more important, to prevent it. In the short run, high quality intelligence gathering and police work are the most critical elements of a successful strategy. But in the long run, encouraging economic and political development is the single most effective counter-terrorism approach, because it is the only one that directly addresses the marginalization, frustration and humiliation of peoples that breeds terrorism, as well as many other forms of violence and inhumanity."*

[1]Interview with Zohrab Gul, Retired Deputy Superintendent of Police, Swat, KP, Pakistan.

[2]For details, please see Police Rules 1934 edited by Ray Zahid Hussain. Lahore: Khyber Law Publishers.

[3]Interview with Zohrab Gul, Retired Deputy Superintendent of Police, Swat, KP, Pakistan.

[4]Interview with Barakatullah, LLB, LLM, Advocate of High Court Peshawar, KP, Pakistan.

[5]Interview with Barakatullah, LLB, LLM, Advocate of High Court Peshawar, KP, Pakistan

[6]Interview with Rahim Shah Khan, Deputy Superintendent of Police, Peshawar, KP, Pakistan.

[7]Interview with Ayub Khan, Superintendent of Police and In-charge of Forensic Science Laboratory, Peshawar, KP, Pakistan.

[8]Ibid

[9]Interview with Naushad Ali Khan, Superintendent of Police, Research, Peshawar, KP, Pakistan.

[10]Interview with Syed Akhtar Ali Shah, Additional Inspector General of Police, Special Branch, KP. Mr. Shah has served as Deputy-Inspector General of Police in Swat and Mardan and has survived two suicide attacks on him.

[11]Central Police Office, Kyber Pakhtunkhwa, Pakistan.

[12]Interview with Zohrab Gul, Retired Deputy Superintendent of Police, Swat, KP, Pakistan.

[13]For details see Fasihuddin. (2008). Identification of Potential Terrorism-The Problem and Implications for Law-Enforcement. *International Journal of Criminal Justice Sciences* (IJCJS). July – December Vol. 3 (2): 84–109.

[14]'Public Prosecutor', means any person appointed under section 492, and includes any person acting under the directions of a Public Prosecutor and any person conducting a prosecution on behalf of the State in any High Court in the exercise of its original criminal jurisdiction. He is bound to assist the Court with his fairly considered view and the Court is entitled to have the benefit of the fair exercise of his function. AIR 1957 S.C. 389.

[15]An Asian Development Bank soft loan to Pakistan is de facto primarily responsible for the Access to Justice Program, in which the state is engaged "in improving justice delivery, strengthening public oversight over the police, and establishing specialized and independent prosecution services? In this we see the Police Act 1861 being replaced by the Police Order 2002 and new laws to constitute and

provide for the functions of independent prosecution services in Pakistan, thus, divorcing prosecution from the investigative arm of the police. Arguably, more valid grounds can be cited for the creation of an independent prosecution service in Pakistan, being article 175(3) of the constitution, which mandates that "the judiciary shall be separated progressively from the executive within three years from the commencing day? Thereafter, there was the appeal decided in Govt. of Sindh v. Sharaf Faridi (PLD 1994 SC 105)

[16]In Sindh, for instance, it was done in 1986; see Zahid, Nasir and Wasim, Akmal, *The province of Sindh as a case study on the prosecution service*: http://www.article2.org/mainfile.php/0704/333/ as on 12 July, 2010.

[17]The laws providing for independent prosecution services are The Sindh Criminal Prosecution Service (Constitution, Functions and Powers) Act, 2009, The Punjab Criminal Prosecution Service (Constitution, Functions and Powers) Act, 2006, The North-West Frontier Province Prosecution Service (Constitution, Functions and Powers) Act, 2005, The Balochistan Prosecution Service (Constitution, Functions And Powers) Act, 2003.

[18]Interview with Iddrees Khan, Deputy Inspector General of Police (Investigation) Peshawar, KPK, Pakistan.

[19]Khan A. J. (Tuesday, June 21, 2011). Nine-year-old would-be girl bomber arrested. In. *The News International*. Retrieved July 12, 2011 from http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=6875&Cat=13

[20]Khan A. J. (Wednesday, June 22, 2011). Mystery continues to shroud arrest. In *The News International*. Retrieved July 12, 2011 from http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=53882&Cat=7&dt=6/22/2011

[21]Reuters. (July 4, 2011). Terror market: TTP sold suicide bomber to Afghan militants. In *Express Tribune*. Retrieved July 21, 2011 from http://tribune.com.pk/story/201828/insurgents-bought-suicide-bomber-from-pakistan-taliban-afghan-spy-agency/

[22]Yasin, A. (May 26, 2011). LEAs Authorised to Use All Means Against Terrorists. In the daily *The News International*. Islamabad, Pakistan.

[23]Burghardt, T. (April 8, 2009). The Political Economy of Taliban Terror in Swat Valley. In *Global Research*. Retrieved July 21, 2011 from http://www.globalresearch.ca/index.php?context=va&aid=13117

[24]Interview with Qazi Hameed, Assistant Director, FIA Headquarters, Islamabad, Pakistan.

References

Amin, A. (April 19, 2011). Only 2% of terrorists are getting sentenced: In Daily *The News International*. Islamabad: Retrieved May 15, 2011 from http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=42426&Cat=7&dt=4/19/2011

Amin, A. (June 6, 2011). Weak prosecution leading to release of terror suspects. In *Daily The News International*. Islamabad, Pakistan.

Bensinger, J. G. (2010). Law Enforcement and Counter Terrorism in Post 9/11 Germany. In *Pakistan Journal of Criminology.* Vol. 2. No. 1. Jan 2010. Peshawar: Pakistan Society of Criminology.

Burghardt, T. (April 8, 2009). The Political Economy of Taliban Terror in Swat Valley. In Global Research. Retrieved July 21, 2011 from http://www.globalresearch.ca/index.php?context=va&aid=13117

Cordner, G., Cordner, M., and Das K. D. (eds) (2010). *Urbanization, Policing, and Security*. New York: CRC Press, Taylor and Francis Group

The Nation. (2009). At least 27 killed, 90 injured in Lahore police training school attack. (March 30, 2009). In The Nation. Islamabad: Retrieved May 15, 2011 from http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/Lahore/30-Mar-2009/At-least-27-killed-90-injured-in-Lahore-police-training-school-attack/1

Dumas, J. L. (2009). The Role of Police Work, Economic Development, and Political Development in Countering Terrorism. In Teymur S., Ozdemir H., Basibuyuk O., Ozer M., and Gunbeyi M. (Eds). *Combating Terrorism.* Washington DC: Turkish Institute for Security and Democracy.

FAFEN. (2011). Pakistan Crime Monitor 2010. Islamabad: Retrieved May 15, 2011 from http://www.fafen.org/site/v1/admin/products/p4d761669cb6b7.pdf

Fasihuddin. (2010). Problems of Data Collection and Constraints in Investigation Management of Cases of Terrorism in Pakistan. In *Pakistan Journal of Criminology*. Vol. 2. No. 1. Jan 2010. Peshawar: Pakistan Society of Criminology.

Ghani, I. (2010). Extremism in Pakhtun Society. In *Pakistan Journal of Criminology*. Vol 2. No. 1. Jan 2010. Peshawar: Pakistan Society of Criminology.

Guiora, N. Amos. (2007). *Global Perspectives on Counterterrorism.* New York: Wolters Kluwer Publishers.

Guiora, N. Amos. (2008). *Fundamentals of Counterterrorism*. New York: Wolters Kluwer Publishers.

Hafeez, M. A. (April 24, 2011). Resources Constraints Hinder Dispensation of Justice. In The News International. Islamabad: Retrieved May 15, 2011 from http://www.thenewstribe.com/2011/04/24/lack-of-resources-cause-delay-in-dispensation-of-justice-cj/

Haider, M. (June 03, 2011). Pakistan Suffers $68b Losses in War on Terror. In *The News International*. Islamabad, Pakistan.

Khurshid, J. (June 27, 2011). Extra Judicial Killings Violations of Law, says Chief Justice. In *The News International*. Islamabad.

Khan, A. J. (Tuesday, June 21, 2011). Nine-year-old would-be girl bomber arrested. In *The News International*. Retrieved July 12, 2011 from http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=6875&Cat=13

Khan, A. J. (Wednesday, June 22, 2011). Mystery continues to shroud arrest. In *The News International*. Retrieved July 12, 2011 from http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=53882&Cat=7&dt=6/22/2011

Khan, A. N., & Sajid, A. I. (2010). Kidnapping in the North West Frontier Province (NWFP). In *Pakistan Journal of Criminology*. Vol. 2. No. 1. Jan 2010.

Makarenko, T. (2003): The Ties that Bind: Uncovering the Relationship between Organized Crime and Terrorism in Siegel Dina, et.al (Editor) *Global Organized Crime*, *Trends and developments*, Kluwer Academic Publisher, London.

Mirza, M. (2010). Role and Responsibilities of the Public Prosecution: A Case Study of Khyber Pakhtunkhwa Province. In *Pakistan Journal of Criminology*. . Vol. 2. No. 3. July 2010. Peshawar: Pakistan Society of Criminology.

Ministry of Population Welfare. (2010). Population Dynamics. Islamabad: Government of Pakistan. Retrieved May 15, 2011 from http://www.mopw.gov.pk/PopulationDynamics By Province.aspx

Naseer, A. (2010). Money Laundering: A Global Threat and Pakistan's Recent Initiatives. In *Pakistan Journal of Criminology.* Volume 2. No. 4. Oct 2010.

Naushad, A. K. (2009). Suicide Bombing in the NWFP: The Need for Research and Information Collection on Human Bombers. In *Pakistan Journal of Criminology*. Vol.1. No.1. April 2009.

Napoleoni, L. (2003). *Modern Jihad: Tracing the Dollars Behind the Terror Networks*. London: Pluto Press.

O'Connell, E. P. (2009). The Chess Master's Game: A Model for Identifying and Classifying Levels of Threats to the Community. In Teymur S., Ozdemir H., Basibuyuk O., Ozer M., and Gunbeyi M. (Eds). *Combating Terrorism.* Washington DC: Turkish Institute for Security and Democracy.

O'Connor, T. (Aug 22, 2010). In *Terrorism and the Law* (Terrorism Investigation), *MegaLinks in Criminal Justice*. Retrieved May 02, 2011 from http://www.drtomoconnor.com/rest.

Osterburg, W. J., and Ward R. H. (2004). *Criminal Investigation, a Method for Reconstructing the Past.* 4th Ed. Ohio: LexisNexis.

Ostrum, E., Parks, R. B., and Whitaker G. (1978). *Patterns of Metropolitan Policing*. Cambridge, MA: Ballinger Publishing Inc.

Oxley, R. M. (March 8, 2006). Why terror financing is so tough to track down? In *Christian Science Monitor*. London: Retrieved July 12, 2011 from http://www.csmonitor.com/2006/0308/p04s01-woeu.html

Pakistan Institute for Peace Studies. (2001). *Pakistan Security Report 2010*. Islamabad: Pakistan Institute for Peace Studies.

Superintendent of Police/ Research, Central Police Office (CPO), Khyber Pakhtunkhwa, Peshawar, Pakistan.

Yasin, A. (May 26, 2011). LEAs Authorised to Use All Means Against Terrorists. In the daily *The News International*. Islamabad, Pakistan.

Yateendra, S. J. (2005). Defeating Terrorism A Study of Operational Strategy and Tactics of Police Forces in Jammu & Kashmir (India): *Police Practice & Research*. Vol. 6. No. 2. May 2005.

The author Fasihuddin (PSP) is a senior police officer in Pakistan. He is also the Editor-in-Chief of Pakistan Journal of Criminology. He can be reached at fasih68@hotmail.com

Are Suicide Bombers Coming from Madaris (Islamic Schools) in Pakistan?

Fashiuddin and Imran Ahmad Sajid

Abstract

This paper studies the association between suicide terrorist and Madaris (Islamic Schools). There is a general myth (at least in the media) that the Madaris in Pakistan are the factories of producing suicide terrorists. After every suicide attack in Pakistan, fingers are pointed towards some unknown tribal Islamic fundamentalist group and the association of the attacker is linked with a Madrassah (singular or Madaris) where he was supposed to be indoctrinated for years to become a holy warrior. We took the secondary data on suicide terrorism from various sources and attempted to answer the sudden rise of suicide terrorism in Pakistan after 2006. We find no primary association between Madaris and suicide terrorism.

Keywords

Suicide, Suicide Terrorism, Attacks, Madaris, Madrassah, Pakistan, History, Islam, Islamic Fundamentalism, Religion.

Introduction

Soldiers fight to protect a cause and sometimes also get killed in the process. However, the suicide terrorists fight by killing themselves to kill others in order to protect the cause. It is a tactic of warfare with such rigour that the world never experienced before. While suicide attacks are not a phenomenon unknown to history, nonetheless, since 9/11 they have received a significant impetus and new dimensions. The recent trend in suicide attacks is alleged with the Madaris (plural of Madrassah, meaning Muslim education institutions, Islamic seminaries). The Madaris are constantly labeled as factories of terrorists and suicide bombers.[1] The Feb 15, 2010 story of one of the leading newspaper of Pakistan—The News—while quoting Dr. Fauzia Saeed, a Social Scientist from Pakistan with a PhD from the University of Minnesota, reported that "Every suicide bomber is coming from Madrassah."[2] Reporting the same seminar, The News severely criticized the role of Madaris in Islamabad. This is not limited only to Pakistan's self defining "progressive" circles but it has become a common norm for the leftists around the world to allege the Madaris for promoting terrorism and producing suicide bombers, though little evidence supports their claims.[3]

In Pakistan, the Madrassah structure was used against the Russian invasion of Afghanistan in last quarter of the previous century. However, during Afghan Jihad, no suicide tactic was used against the Russians. Nonetheless, the suicide attacks are used against the US and allied forces in Afghanistan as well as in Pakistan—against

the security forces and also against the civilians. Now that the Madaris were used against Russia and the students of the Madaris were made into holy warriors, it is quite logical to assume that the same Mujahideens (holy warriors) who battled against Russia are also fighting against the US. In this process, they are using every mean to compel US to withdraw its forces from a land they consider as their own. Suicide attack is one of these means utilized by the supposed Mujahideens who were produced by the Madaris (See Box 1 for the logical relationship).

At first glance, the conclusion seems valid. However, a little more depth of analysis and reasoning arises numerous questions regarding the claim. Why were Madaris not opting for suicide attacks against Russia but are using against US and NATO forces? Besides this, a more fundamental question one would ask is that are the Madaris really involved in producing suicide bombers? Is there any actual link between suicide terrorists and Madaris? Does the research support the common perception? These are a few questions which this paper will discuss. Before taking them into full consideration, we need to understand the background of Madaris in the Muslim world in general and in Pakistan in particular.

Box 1: Madaris - Suicide Logical Relationships

Madaris	⇢	Produced	⇢	Mujahideen
Mujahideen	⇢	Fought	⇢	Russia
1. Madaris Fought Russia				
Mujahideen (Madaris)	⇢	Fought	⇢	Russia
Russia	⇢	Replaced by	⇢	US
2. Mujahideen (Madaris) Fight US				
Mujahideen (Madaris)	⇢	Fight	⇢	US
Suicide Terrorist	⇢	Target	⇢	US
3. Madaris Produce Suicide Terrorist				

Uzma Anzar informs the readers to understand the difference between a Madrassah and a Maktab. For her, a Maktab (or a Koranic School) is a place where Muslim children go to read and recite only the Koran (also spelled as Quran or Qur'an). She adds that a Maktab can function in varying environments, in mosque, under a tree, in the house of the Koran teacher or under an open sky. [It needs to be

be added here that each and every mosque, in general, in the Muslim society functions as a Maktab, providing only the facility of reading and reciting the Koran, even if the children do not understand it]. The term Madrassah, for Uzma Anzar, is used for a bit more organized institutions with classrooms and teachers for different levels. Many Madaris, she adds, provide boarding facilities for students free of charge. [The term, Darul Ulum is also sometimes used for Madaris]. In other words, a Madrassah is an institution of advance studies in Muslim societies while a Maktab teaches only the basic skills of reading and reciting the Koran.[4] The term Madrassah is derived from Dars (درس) which means to learn, therefore, the official reports of the Ministry of Education, Islamabad, Pakistan use the term Deeni Madaris to describe the Islamic schools in Pakistan because a Madrassah literally means any learning institution, both secular and religious.

History of Madaris

Acquiring knowledge has a significant position in Islam. Muslims are encouraged to acquire knowledge and for this purpose there are no geographical boundaries. One of the Hadith (sayings of the Holy Prophet Muhammad (SAW)) states that "seeking of knowledge is the duty of every Muslim (man and woman)." In the initial years of Islam, the teachings of Koran and Hadith were being imparted through the mosques. However, as Islam started to expand gradually throughout the East and the West of Arab, it became necessary to cater for the needs of the non-Arab Muslims for religious knowledge and understanding. Thus, a cadre of Muslim experts was created who would develop sophisticated writings and textbooks on Fiqa (Islamic jurisprudence), Sunna (Prophet's traditions), Hadith (Prophet's sayings), and Tafseer (the interpretation of the Koran). It began the tradition of Madrassah, the center for higher learning the initial purpose of which was to preserve religious conformity through uniform teachings of Islam for all.[5]

The first proper Madrassah was established by the Saljuk minister Nizam-ul-Mulk Tusi in Baghdad in the year 1067.[6] Tusi introduced two types of education in this Madrassah: scholastic theology to produce spiritual leaders, and earthly knowledge to produce government servants. Similar kind of Madaris were later established by Tusi all over the empire which, in addition to imparting Islamic knowledge also imparted education in varying fields such as science, philosophy and public administration and governance. Haqqani credits Nizam-ul-Mulk to be the father of the Islamic public education system.[7] Further, Tusi himself is the author of a renowned book (among early Muslims) on public administration called Siyasat Nama (the way to govern).[8]

For much of the later centuries, the Madrassah system remained unchanged, produced numerous renowned scholars both in religious and secular fields. e.g. Ibn Rushd, the mathematicians, al-Zarqali and al- Bitruji, and the physician Ibn Zuhr,

Al-Ghazali, Ibn Sina and Ibn Khaldun to name a few. However, with the gradual decline of Muslim world by the hands of Crusaders, Mangols, and later, by European colonization, the Muslim scholarship also went into a decay, resulting in closing of the door to Ijtihad (independent reasoning).[9] However, the Indian Sub-continent was one of the many regions where the Muslim Madaris went through a radical shift.

Indian Sub-continent and Madaris

One editorial paper by Jamiatul Uloom-ul-Islamia, Banuri Town, Karachi, finds out that before the arrival of the East India Company to the Indian Sub-continent, Madrassah education was the only formal means of educating the Muslim masses. Delhi, Agrah, Lahore, Multan, Jonpure, Lakhnaw, Kherabad, Patna, Ajmer, Deccan, Madras, Bengal and Gujrat were the famous cities for their advance institutions of education. The paper also finds out that "before the arrival of the British to Bengal, there were about eighty thousand (80,000) Madaris in Bengal, which averages at 400 populations per Madrassah."[10] Similarly, in the times of Muhammad Shah Tughlaq, there were 1,000 Madaris in the city of Delhi.[11] The source of income for these Madaris was the properties allotted to them by the Nawabs (local rich and royal chief) etc. However, with the arrival of British and their commitment to introduce an alternative system of education in India, the old system of Madaris gradually started disintegrating. Particularly, the 1857 war of independence brought a very hard time on Madaris in the Indian Sub-continent as Madaris were alleged for producing Mujahideens (holy fighters) for this war.[12]

The education system, which is prevalent in Indian and Pakistani Madaris today, was devised by Mullah Nizam-ud-Din Sihalvi (1747), Lakhnaw, India. The curriculum he devised included twenty one (21) different subjects. Medicine, Physics, History, Geology and Mathematics were compulsory subjects. However, these very important subjects are taught nowhere in Madaris in India or Pakistan today. Further, the curriculum consisted of seventy two (72) renowned and authentic books on these subjects (See Table I for details of subjects and books).[13]

After the war of independence in 1857, Maulana Qasim Nanotvi established Madrassah Deoband at a small village in Soharanpur district in 1867. It was the first formal Madrassah establishment after 1857. It was different though. The Madaris before the British arrival were funded by the Nawabs.[14] However, Dar-ul-Uloom Deoband was funded through public charities and donations. The other difference, though no reference is available for this, was that this new Madrassah imparted only the religious knowledge to the students. The secular education was left to the British education system. This was the beginning of the present environment which prevails throughout majority of the Madaris in India and Pakistan. This radical shift in

Madaris education in Indian Sub-continent reduced the influence the Ulema (religious scholars) had on the society. Further, the role of Madaris was significantly reduced. Their graduates were excluded from government employment and there was very little substitute for this.[15]

The reason for this "pauperization" of Madaris needs to be researched in details. In brief, on the one hand, the British missionary policy of Christianization of the masses through missionary schools and colleges created fear amongst the Muslim Ulema about the future of the faith. While on the other hand, preservation of the religion as a duty compelled them to take steps and revert to the very basics of the religion. The picture seems to be similar to as when the Mongols started conquering the Muslim states. At that time, the same happened. The Madaris reverted to the very basics of the religion and the doors of Ijitihad were closed down. Mufti Taqi Usmani also concludes that the secularization of educational policies of the British in India and the bias towards religious education created a stir in the Muslim scholars. They feel apprehensions over the future of religious teachings. This was the reason why the education system was divided into two: religious and secular, by Muslims of the sub-continent.[16]

This brief historical picture concludes that whenever the Muslim society is under invasion from another force, it reverts to the very basics. Table I puts some more light on this thesis. It is obvious from the table that along with religious subjects, the secular subjects were also part of the curriculum of Madaris in Dars-e-Nizami (the curriculum of Nizami). Logic, Philosophy, Mathematics, Medicine, Physics, and History were part of the curriculum. However, much of these subjects have been excluded today, particularly after the 1857 war of independence, the Madaris reverted to the very basic subjects of the curriculum—Serf-o-Nahw (Arabic Grammer), Fiqh, Tafseer, Hadith etc—because of the perceived threat to the faith. It is pertinent to note that out of these seventy two (72) books, neither a single book mentions any teaching on suicide jihad / suicide terrorism nor the subjects promote radicalism. Similarly, never in history the Madaris in Indian Sub-continent were ever used as a safe-heavens for terrorists.

S. No.		Subject	Books	Author	Year of Publication (Hijri)
1	1	Serf - o - Ishtiqaq - e - Arabi (Arabic Etymology)	Meezan - us - Serf	Muhammad bin Mustafa bin Al - Haj Hassan	911
	2		Manshab	- do -	
	3		Punj - Gunj	- do -	
	4		Serf - Meer	Mir Syed Sharif Al-Jarjani	816
	5		Ilm - us - Seegha	Mulana Mufti Inayat Ullah	1277
	6		Fasool - e - Akbari	Qazi Muhammad Akbar	N/A
2	7	Arabi Nahw (Arabic Grammer)	Nahw - e - Meer	Mir Syed Sharif Al-Jarjani	816
	8		Sharh - e - Matul Amil	Mullah Muhammad Sadiq Al-Jarjani	1190
	9		Hadyat - un - Nahw	Abu Hayyan Nahwi	745
	10		Kafya	Imam Jamal-ud-Din ibn Hajab Nahwi	620
	11		Sharh - e - Jami	Mulana Shiekh Abdur Rehman Jami	850
	12		Sharh - e - Ibn - e - Aqeel Ali Alfye - Ibn - Malk		887
3	13	Balagha (Rhetoric)	TalKhees - ul - Miftah	Allama Jalal - ud - Din Muhammad bin Abd - ur - Rehman Qazwini	739
	14		Mukhtasar - ul - Ma'ani Sharh - e - TalKhees - al - Miftah	Saad ud Din Taftazani	792
	15		Matlool Sharh - e - Talkhees - ul - Miftah	do	do
4	16	Arooz-o-Qawafi (Geography)	Arooz-ul-Miftah	Abu Ayyub Sakaki	626
5	17	Mantiq (Logic)	Sughra-o-Kubra	Mir Syed Sharif Al-Jarjani	816
	18		Eisa Ghoji	Aseer-ud-Din Abhari	661
	19		Sharh-e-Tahzeeb Taftazani	Abdullah Yazdi	981
	20		Sharh-e-Shamsya (Qutbi)	Qutb-ud-Din Razi	866
	21		Salm-ul-Ulum	Muhibullah Bihari	1119
	22		Risalah Mir Zahid	Mir Muhammad Zahid Haroi	1101

S. No.		Subject	Books	Author	Year of Publication (Hijri)
6	23	Falsafa (Philosophy)	Sharh - e - Mibzi Alal Hidayat - ul - Hikmah	Mir Hussain Mibzi	1092
	24		Sharh - e - Sidra	Muhammad bin Ibrahim Sadrud Din Shirazi	1050
	25		Shams Bazigha	Mullah Mehmood Junpuri	1062
7	26	Adab - e - Arabi (Arabic Literature)	Maqamat - e - Hariri	Abu Muhammad Qasim bin Ali Hariri	516
	27 28		Deewan - e - Mutanabba	Ahmad bin Hussain Abu al - Taib Mutanabba	400
	29		Deewan - e - Hamasa	Abu Tamam Tai	222
			Sibgha - e - Mualiqah	N/A	N/A
8	30	Tareekh (History)	Tareekh - e - Khulfah	Allama Jalal - ud - Din Muhammad Sayuti	981
	31		Tareekh - e - Abi Al - Fida	Abu-al-Fida Hamudi	742
9	32	Aqaid-o-Kalam (Theology)	Sharh-e-Aqaid-e-Nasfi	Saad - ud - Din Taftazani	762
	33		Musafirah	Kamal - ud - Din ibn Alham	905
	34		Khyali	Shams - ud - Din Khyali	870
10	35	Tib (Medicine)	Al-Mojaz	Abul Hassan ibn Al-Nafees	687
	36		Qanooncheh	Muhammad bin Umar Chaghmini	8
	37		Hamiyatul Qanoon	Sheikh Bu - Ali Seena	427
	38		Sharh - ul - Asbab	Burhan - ud - Din Nafees bin Ewaz Karmani	827
11	39	Heyyat (Physics)	Al-Tasreeh	Imamud Din bin Lutfullah Lahori	1145
	40		Sharh-e-Chachmini	Musa bin Mehmood Qazizada	814
12	41	Hindsah (Mathematics)	Bast Bab	Naseer-ud-Din Muhaqiq Alvi	672
	42		Aqleedas	Abul Hasssan Tsabi bin Qurrah	289
13	43	Munazrah (Polemics and Debate)	Risalah Rashidya	Shams - ul - Haq bin Sheikh Abdur Rashid	1080
14	44	Fiqh (Jurisprudence)	Noor - ul -Izah	Hassan bin Ali Sharbnali	1196
	45		Mukhtasar-ul-Qudoori	Abul Hassan Qudoori	428

S. No.		Subject	Books		Year of Publication (Hijri)
14	46		Kanzud Daqaiq	Abul Barkat Nasfi	470
	47		Sharh-Wiqaya	Sadr - us - Shariah Ubaidullah bin Masood	543
	48		Hidayah	Burhan-ud-Din Ali Murghyani	573
15	49	Asool - e - Fiqh (Basics of Jurisprudence)	Asool - e - Shashi	Nizamud Din Shashi	754
			Noor-ul-Anwar Sharh-e-Alminar	Sheikh Ahmad Mullajyoon	1105
	50		Mukhtasar - ul - Hassami	Hassamud Din Muhammad bin Muhammad bin Umar	644
	51		Al - Todeeh	Sadr - us - Shariah Ubaidullah bin Masood	543
	52				
	53		Al -Talweeh	Saad - ud - Din Taftazani	792
	54		Muslim - al - Saboot	Muhibullah Bihari	1119
16	55	Meeras—Faraiz (Inheritance Law)	Mukhtasar - ul - Siraji	Sirajud Din Sajawandi	N/A
	56		Sharifyah	Syed Sharif Jarjani	816
17	57	Asool - e - Hadith (Basics of Hadith)	Sharh - e - NaKbat - ul - Fikr	Hafiz ibn Hajr Asqalani	852
18	58	Hadith (Traditions)	Mishkat-ul-Masabih	Sheikh Waliud Din Iraqi	
	59		Jami-ul-Bukhari	Imam Muhammad bin Ismail Bukhari	252
	60		Sahih Muslim	Imam Muslim bin Hujaj Qashiri	261
	61		Jami-Tirmizi	Imam Muhammad bin Eisa Tirmizi	279
	62		Sanan Abi Dawood	Imam Abu Dawood Sulaiman bin Ashas	275
	63		Sanan Nasai	Imam Ahmad bin Shoib Nasai	206
	64		Sanan Ibn-e-Maja	Imam Abu Abdullah Muhammad bin Majah	273
	65		Kitabu-Shimail	Imam Abu Eisa Muhammad bin Eisa Tirmizi	279

S. No.		Subject	Books		Year of Publication (Hijri)
	66	Hadith (Traditions)	Sharh - e - Muani - ul - Asar	Imam Abu Jafar Ahmad bin Muhammad Slamo Tuhawi	361
	67		Almota	Imam Malik bin Ans	179
	68		Almota	Imam Muhammad bin Hassan Sheebani	N/A
19	69	Tafseer (Commentary of Quran)	Tafseer - e - Jalalain	Jalalud Din Sayuti & Jalalud Din Mahli	981
	70		Anwar - ut - Tanzil	Qazi Abdullah bin Umar Bidhavi	716
	71		Midrak - ut - Tanzil	Imam Najmud Din Umar Nasfi	753
20		Asool - e - Tafseer (Basics of Commentary of Quran)	Al-Fozul Kabir fi Asool-e-Tafseer	Imam Shah Waliullah Dehlwi	1172

Pakistan and Madaris — a Deep Rooted Relation

The Madaris system in Pakistan is not much different from the pre-independence system. Even after the creation of Pakistan in 1947, the role of Madaris remained restricted and the doors for government employment were still closed to their graduates.[17] The objectives of the religious institutions remained the same as they were under British rule in India: preparing imams (leaders) for mosques, teachers for schools, orators for weekly sermons, and religious leaders to carry out rituals and social responsibilities such as nikah (marriage contracts), divorce, inheritance, and funerals.[18]

However, Akhtar Ali Shah, a senior police officer of Pakistan, sees Madaris as deeply intertwined part of the social fabric of Pakistani society. After an historical analysis of the role of Madaris in the politics of Pakistan, he concludes that Madaris have been providing livelihood, education, and essence of identity to those millions who happened to be the sons of lesser gods.[19] Prakhar Sharma also holds the similar view. According to him, the people of Afghanistan [and Pakistan] consider Madrassah and religious scholars to be integral parts of their history and identity, but the West generally views them as a breeding ground for extremists.[20]

Statistics on Madaris in Pakistan

According to the Ministry of Education 2008 report, there were a total of 12,448 Deeni Madaris in Pakistan.

Table II: Details of Madaris and Teacher/Student Enrollment in Pakistan 2008

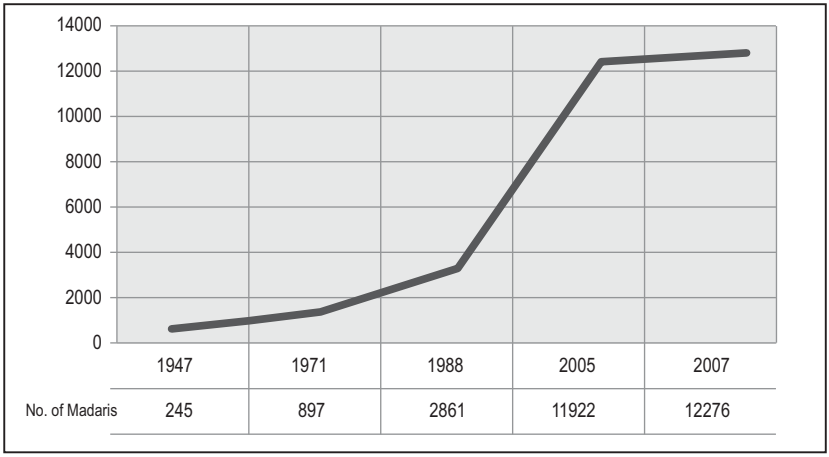
Type of Madaris		Teachers			Students		
		Male	Female	Total	Boys	Girls	Total
Public	321	1,189	351	1,540	25,049	15,143	40,192
Other Public*	42	119	35	154	3,247	1,963	5,210
Private	12,085	41,689	12,297	53,986	971,343	587,211	1,558,554
TOTAL	12,448	42,997	12,683	55,680	999,639	604,317	603,956

Source: Pakistan Education Statistics 2007-08. Academy of Educational Planning and Management, National Educational Management Information System, Ministry of Education, Islamabad, Pakistan.
*Other Public are those institutions which are public but are not run by Ministry of Education/provincial or federal.

There were a total of 12,448 Deeni Madaris in Pakistan in 2008, of which 363 (3%) are in public sector, whereas 12,085 (97%) are in private sector. The total enrolment in the Deeni Madaris is 1.603 million of which 0.454 million (3%) are in public sector, whereas, 1.558 million (97%) are in private sector. The total male enrolment in Deeni Madaris is 0.999 million (62%), whereas, the female enrolment is 0.604 (38%). The total teachers in Deeni Madaris are 55,680, out of which 1,694 (3%) are in public sector and 53,986 (97%) are in private sector. There are 42,997 (77%) male teachers and 12,683 (23%) female teachers (See Table II for details).

When Pakistan came into being in 1947, the presence of Madaris was very limited as compared to today. However, as the time moved on to 1971, the Madaris rose upto 897, only 72% increase in 24 years. During the next 17 years there was also a significant increase in Madaris, i.e. 68% increase. Astonishingly, there was 76% increase in Madaris between 1988 and 2005. Graph I shows a normal increase in number of Madaris between 1947 and 1988. However, the curve suddenly moves upward during 1988 and 2005. Why this sudden rise in Madaris? It is always attributed to the Afghan-War against the Soviet Union during 80s and the successive Taliban rise to the power in Afghanistan during 1996-2001.

Graph I: Details of Madaris in Pakistan (1947-2007)



(1)Pakistan Education Statistics 2007-08. Academy of Educational Planning and Management, National Educational Management Information System, Ministry of Education, Islamabad, Pakistan.
(2) Syed Akhtar Ali Shah. (2011). The Role of Madrassahs (Islamic Seminaries) in the Politics of Pakistan. Pakistan Journal of Criminology. Vol.3.No.1.Jan 2011.pp.9-34.
(3) M.Taqi Usmani (1989, 2005). Our Education System [Hamara Nizam-e-Taleem Kya Hua] Urdu. Karachi: Maktaba Darul Uloom. pp.71-73

Out of the total 12,448 Madaris, only 321 (3%) are in Public sector while 97% are in private sector. The private Madaris are imparting education to a total of 1,558,554 students out of which 971,343 (62%) are boys while only 587,211 (38%) are girl students, which is not significantly different than the educational enrollment in public sector schools and colleges (about 44% girls in all schools). Teacher students' ratio is 1:28 at average. The number of registered Madaris is only 6,803 (55%).[21] It is pertinent to mention here that the Madaris also give admission to the foreign students. According to one report of the Ministry of Interior, there were 2,606 foreign students in Madaris of Pakistan in the year 2005.[22]

The province-wise break-up of Madaris also presents an interesting picture. A significant number of Madaris are located in the Punjab (44%) followed by Khyber Pakhtunkhwa (KP) 21%, and Sindh 15%. There is a very small number of Madaris in Balochistan. FATA, with a population of 3,341,070, contains 498 Madaris, which makes it one (1) Madrassah for every population of 6,709 numbers of people, compared to 14,956 in Punjab, 16,327 in Sindh, 1,1420 in Balochistan and 7,976 in KP[23] It is easy to infer that there are more Madaris per population in FATA and KP than the other provinces of Pakistan (see Table III: for details).

Table III: Province - wise Details of Madaris Teacher / Students Enrollment 2008

Province/Area	Institutions				Enrollment		
	Male	Female	Mixed	Total	Male	Female	Total
Punjab	2,018	1,072	2,348	5,438	424,363	274,635	698,998
	47%	54%	38%	44%	42%	45%	44%
Sindh	493	143	1,226	1,862	196,079	120,585	316,664
	12%	7%	20%	15%	20%	20%	20%
KPK*	1,197	476	960	2,633	247,632	107,575	355,207
	28%	24%	15%	21%	25%	18%	22%
Balochistan	214	28	441	683	45,226	23,371	68,597
	5%	1%	7%	5%	5%	4%	4%
AJK **	158	160	862	1,180	43,735	49,041	92,776
	4%	8%	14%	9%	4%	8%	6%
Gilgit - Baltistan	44	6	42	92	10,861	3,002	13,863
	1%	0%	1%	1%	1%	0%	1%
FATA***	130	71	297	498	27,155	19,715	46,870
	3%	4%	5%	4%	3%	3%	3%
ICT ****	24	14	24	62	4,588	6,393	10,981
	1%	1%	0%	0%	0%	1%	1%
Grand Total	**4,278**	**1,970**	**6,200**	**12,448**	**999,639**	**604,317**	**1,603,956**
	100%	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Source : Pakistan Education Statistics 2007 - 08. Academy of Educational Planning and Management, National Educational Management Information System, Ministry of Education, Islamabad, Pakistan.

* Khyber Pakhtunkhwa

** Azad Jammu and Kashmir

*** Federally Administered Tribal Area

****Internal Capital Territory

Note that FATA and KP are the regions which are severely hit by suicide terrorism. Further, these two are the Pashtoon dominant regions as well. It may seem fit to jump to the conclusion that the more the Madaris the more the suicide attacks in the region. However, it is very naïve and seems over-simplification. This point will be discussed later in details.

Madaris Degree and Awards Systems in Pakistan

The level of Madaris education system corresponds to the levels of mainstream state education in Pakistan (see Table IV for details of Madaris curriculum and levels). The first five years of a child are busy learning to read the Koran, i.e Nazirah, simple recitation. It is equal to the Primary or 5th grade education in Pakistan. The Hifz or learning to memorize the Holy Koran by heart takes about three years and is equivalent to 8th grade education of the mainstream state educational level. Next comes the Tajveed and Qirat, i.e. recitation of the Koran in an accurate Arabic accent and in a beautiful tone which takes about two years to complete and is equivalent to a Secondary School Certificate educational level of the state. The Higher Secondary degree is termed as Thanviyah-Khassa while the Aliya is the graduate level degree and takes 13 to 15 years of overall education to complete.

Table IV: Curriculum in Deeni Madaris in Pakistan

Level (Darja)	Level	Class	Duration	Certificate (Sanad)	Certificate (Sanad) Comparable to Mainstream Education
Ibtidaya (Primary)	Nazara (Recitation)	01 - 05	4 - 5 yrs	Shahadatul Tahfeez ul Quran	Primary (5th Grade)
Mutawassitah (Secondary)	Hifz (Memorization)	06 - 8	3 yrs	Shahadatul Mutawassitah	Middle (8th)
Thanviyah - e - Ammah (General Middle)	Tajveed, Qirat (Recitation with style and accent)	Ulla va Thanviya (9, 10)	2 yrs	Shahadatul Thanviya ul Amma	Matric (10th)
Thanviyah - e - Khassah (Special Middle)	Tehtani (Higher Secondary)	Arbiat va Ashara (11, 12)	2 yrs	Shahadatul Thanviya ul Khaassaah	Intermediate (F. A.)
Aliya (Higher)	Mohqufaleh Khasa va Sada (College)	Arbiat va Ashara (13, 14)	2 yrs	Shahadatul Aliya	B. A.
Alamiya (Highest)	Daura Hadiths Sabia va Sanniya	Master phil Arabic phil Uluum al Islamia (15, 16)	2 yrs	Shadatul Alamiyah phil Uluum ul Arabia vul Islamia	M. A. recognized as such, in Arabic and Islamic Studies by government
Takmeel (Completion)	Post Graduate	Varies with specialization	1 yrs	Varies with specialization	Post - M. A.

Source: Ayesha Jalal. (2008). Partisans of Allah: Jihad in South Asia. Lahore: Sang-e-Meel Publication.

Alamiya, a more general degree of Madaris, is equivalent to the post graduate or M.A. degree of the mainstream state education. It is pertinent to note that an Alamiya degree holder is given an equivalence certificate by the state which is equal to M.A. in Islamiat (Theology or Islamic Studies) or Arabic from a University. Besides this, there are also others courses for different competence and professional sections like Molvi Fazil course, Mufti Course, and Imam Course. However, no study has taken these courses of Islamic education into their discussion.

Suicide Terrorism, Religious Motivation and Madaris in Pakistan

The Question: Is there any association between Madaris and Suicide Terrorism?

With every suicide bombing in Pakistan, fingers are pointed towards the possibility of a relationship between the bomber and an Islamic school, Madrassah.[24] Usually a young boy of 13-18 is suspected to have done the deadly blast who, in the educated guess and considered opinion of the investigation staff, is said to have had some links with the tribal groups as the sketch being prepared by the officer in light of the statements of eye-witnesses is reportedly indicative of his ethnicity and background. A more general depiction of the story is like this:

- A hand/foot/skull is found from the scene of crime
- Footage from CCTV/mobile attained
- Young boy, 12-14, 15-17seen and suspected
- White clothes, new shoes, beads in hands, white cap/turban/hanki on head
- Small beard, medium height
- Afghani, Tribal, or Pushtoon by appearance
- Sketch prepared from eye-witnesses and footages / videos
- Probably a student of Islamic Madrassah

This is the most common practice of our media and investigation staff in Pakistan to fix the responsibility on some unidentified suicide bomber, who is reported to be a religiously motivated tribal or Afghani, with a tender age and in most probability being radicalized in some Islamic school of an unidentified place, and furthermore, some unknown Islamic school master (s). This is generally believed and released to the media even before any forensic sciences applications, laboratory tests or tracing police criminal record or national identity card data base.[25] This practice saves the police from many hurdles and fatigue of cumbersome investigation, as police of the cities have no authority and jurisdiction in the Pakistan's tribal territories. Moreover, the propaganda against Madaris is trumpeted

so vehemently to the tune of those who want a ready scapegoat in the long war on terror. Madaris or some radical militant Islamic fundamental groups are the first to be blamed for carrying out suicide terrorism. However, is there any relationship between suicide terrorism and the Madaris? Is it the Madrassah structure and system which promotes suicide terrorism? Is this a common norm in Madaris to carryout suicide terrorism? Do the data support the same claim?

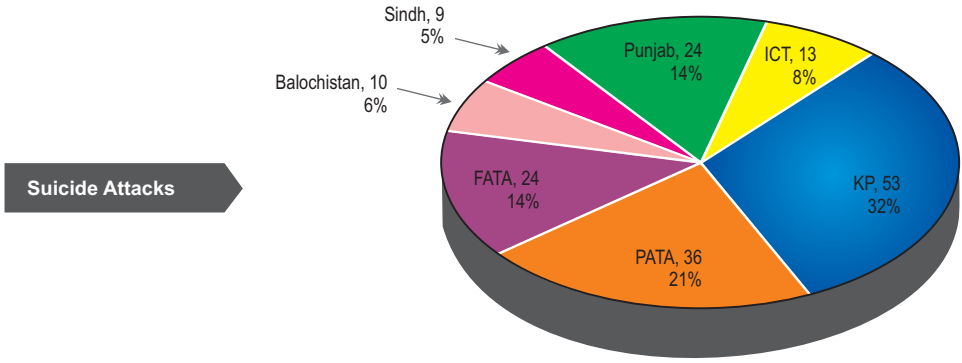
The Findings:

Association between Madaris and Suicide Terrorism

As we discussed earlier that the more the Madaris the more will be suicide attacks in the region is too simplistic to conclude. It is visibly found that KP and FATA share more number of available Madaris for population than the other parts of the country(498 Madaris, which makes it one (1) Madrassah for every population of 6,709 numbers of people and in FATA, 7,976 for KP).[26] Similarly, Graph II shows that KP and FATA are the two regions which are severely hit by the suicide attacks. KP with a total of 53 suicide attacks between 2002 and 2009 shares 31% of all attacks followed by 24 attacks in the Punjab and 9 attacks in Sindh. However, FATA and PATA[27] also experienced 24 and 356 attacks respectively. Ethnically, both FATA and PATA are predominantly Pashtoon regions. Further, these are the regions where military has started to move in post 9/11 scenario. Never in history, before 9/11, KP, FATA, or PATA had ever experienced any suicide terrorism. In post 9/11 scenario, they did, however, experienced them more severely than anywhere else in the world. The question still remains why in post 9/11? The answer is in Robert Papes findings which we will discuss later.

For the time being, the point of focus here is that first, in Table II, we said that there were 1.6 million students enrolled in *Deeni Madaris* in Pakistan in the year 2008. Secondly, there were a total of 303 suicide attacks in Pakistan since 2002.[28] Astonishingly, 12,448 Madaris with 1.6 million of enrolled students are producing only 303 suicide bombers in a decade! The facts denounce the claim of suicide bombers coming from Madaris or religious motivation is seen in all suicide bombers. Holmes, while analyzing statements issued by Al-Qaeda, has emphasized that Osama bin Laden's rationale for 9/11 has usually been secular rather than religious, focused towards 'punishing Western injustices, not impieties'.[29]

Graph II: Suicide Attacks in the Administrative Units of Pakistan



Source: Dr. Muhammad Irfan and Zeeshan-ul-Hassan Usmani. (2011). Suicide Terrorism and its New Targets—Pakistan. In Unaiza Niaz (eds). Wars, insurgencies, and Terrorist Attacks, a Psychosocial Perspective from the Muslim World. Karachi: Oxford University Press. pp.78-9.

Holmes' conclusion also stands valid when we analyze the statements of one of the suicide bombers, arrested before detonating himself in Lahore. He said that he became suicide bomber when he saw the military operations in Lal Masjid (Red Mosque) and Bajur, meaning his motivation was not to bring Islam or Shariah (Islamic Law) but to take revenge against the injustices of the military.[30] In the same interview, the suicide bomber revealed that none of his batch-mates at the training center at Miran Shah were from the Deeni Madaris, all were from the secular schools.[31] The KP police also revealed the same findings through investigation.[32]

Similarly, the religious scholars, at least in Pakistan, denounce suicide attacks. The supreme religious leader of Pakistan, Mufti Munib - ur - Rehman, who is also the Chairman Royat - e - Hilal Committee, issued that

> *"Fighting in the way of Allah, for the uplift of religion, for the superiority of right things, giving your life, and when the time comes participating in Jihad, showing courage, vigilantism, and gallantry are not only valid in Islam but in the time of need it is also termed the Superior Prayers (Afzal Ibadat) and have superior degrees for the life hereafter. But vigilantism and gallantry is that when you come to the battle field and fight, sometimes you also got killed but you do not start the battle with killing*

yourself first. In suicide attack, the attacker begins by killing himself and his own person, any valid argument for this has not come into my knowledge and to the extent I know the religion, I never came across any such justification from Quran and Hadith." [translated from Urdu] [33]

While Mufti Munib is from the Barelvi school of thought (which are considered religious liberals), the Deobandi School (a relatively religiously conservative school of thought) also denounces suicide attacks. One of the most influential Deobandi clerics of Pakistan, Maulana Hasan Jan, while signing a fatwa (decree) against suicide bombing in Pakistan, described the perpetrators as 'cruel and ignorant people', and that these people have 'no knowledge and education'. He said that suicide bombing was haraam (forbidden) and against the Shariah, and added that the situation in Afghanistan and Iraq was different from Pakistan. He concluded: 'We are completely against suicide activities in our country.'[34] However, later on, Maulana Hasan Jan was killed in a terrorist attack on September 17, 2007 in Peshawar.

Analyzing the data over the past thirty years (30) Pape asserted that religion is neither an essential, nor a sufficient factor in the generation of suicide attacks and the taproot of suicide terrorism is nationalism not religion.[35]

Christine Fair discusses the connection between Madaris and militancy to a greater length in her book, The Madrassah Challenge. While remaining impartial, she argues that evidence counters the most sweeping contemporary claims that Madaris are extensively involved in the production of militants in Pakistan and elsewhere. In her study of 141 militant families in Pakistan and find out that only 19 were reportedly recruited from Madaris. Less than a quarter of the militants (33 of 141) ever attended a Madrassah. Of those thirty-three 27 attended a Madrassah for four or fewer years, and most also attended public schools. Eighty-two out of 141 were well educated on Pakistani standards (at least tenth grade).[36] These findings indicate that the militants in general are not uneducated or from Madaris. While Christine Fair tried to find an association between Madaris and militancy, she failed to consider the presence of military or foreign occupation as the essential condition for suicide terrorism.

Moreover, Naushad Ali Khan, a police officer in Khyber Pakhtunkhwa Police department, and Superintendent of Police (Research), finds out that none of the 'living bombers' (those who couldn't blow themselves up and got arrested), had exclusively religious education. Only 10% had only secular education and 90% had both religious and secular education. Further, not all but majority were from tribal origin (70%), a predominantly Pashtoon territory.[37]

Finally, Papes conclusion remains significantly valid that 'religions do play a role in suicide terrorism, but mainly in the context of national resistance.'

Why Suicide Attacks?

The Answer:

Foreign Occupation not Islamic Fundamentalism

Since independence of Pakistan in 1947, not a single suicide terrorist attack was ever recorded. The first known suicide attack in Pakistan was carried out on Nov 11, 1995 on Egyptian Embassy, Islamabad. A suicide bomber rammed a pickup truck packed with explosives into the gate of the Egyptian Embassy in Islamabad, killing 15 people and wounding 59 others. There were no other suicide attacks during 1995 and 2002.[38] The present bloom of suicide attacks in Pakistan grew after the US invasion in Afghanistan.

The director of the Chicago Project on Security and Terrorism (CPOST) and the author of the book, Dyeing to Win: The Strategic Logic of Suicide Terrorism and Cutting the Fuse: The Explosion of Global Suicide Terrorism and How to Stop It, Robert Pape presented his thesis that religion is not the basic motivation of suicide terrorism and that the Islamic Fundamentalism is not the cause of suicide terrorism.

He finds out that during the period 1980 to 2003 there were 343 completed suicide terrorist attacks. About 88% of these attacks had ideological affiliations. The world leader (in terrorist attacks) during this period is not an Islamic group but are the Tamil Tigers of Sri Lanka—a Marxist group, a secular group, a Hindu group. The Tamils in Sri Lanka did more suicide attacks (78 suicide attacks) than Hamas or Islamic Jihad in Israel. The other group of suicide attacks is the PKK of Turkey, which is purely a secular Marxist, anti-religious suicide terrorist group, which carried out 14 suicide attacks in Turkey. Over 50% of these suicide attacks were not associated with Islamic fundamentalism (See Table V).

Table V: Suicide Terrorism Attacks World-wide (1980 - 2002)

Total Suicide Attacks	343
Ideological Affiliations	298
Tamil Tigers in Sri Lanka	78 Attacks
PKK in Turkey	14
Al - Aqsa Brigade	25
Popular Front for the Liberation of Palestine (PFLP) on West Bank	6
Syrian Social Nationalist Party (SSNP)	8
Baa'th Party in Lebanon	8

Source: Robert Pape - Cutting the Fuse The Explosion of Suicide Terrorism and How to Stop It (1 of 4). Retrieved Feb 1, 2012 from http://www.youtube.com/watch?v=Gp17H7aIYNA

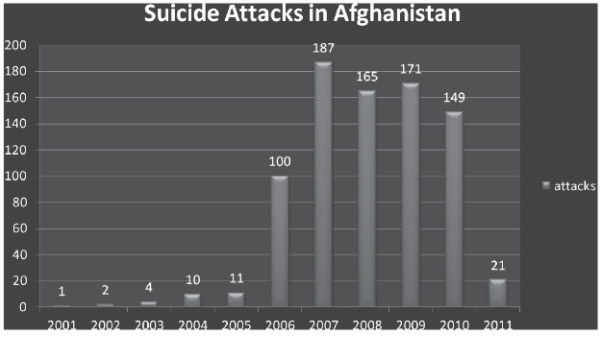
He questions the myth of suicide terrorists coming out of Islamic fundamentalism on the basis of data and argued that what most people think is that suicide terrorism is driven by religion, particularly Islamic fundamentalism. However, the data negates it. The facts don't fit. What is common in 95% of the world-wide suicide terrorist attacks is not religion, but a specific strategic objective to compel democratic forces to withdraw combat forces from the territory the terrorist consider to be their homeland. From the Lebanon to the West Bank to Chechnya and Iraq and Afghanistan today, every suicide terrorist campaign has been waged by terrorist groups for this strategic objective. It doesn't account for every suicide attack, it does, however, account for over 95% of the attacks of all the suicide terrorism we have experienced since 1980.

The point to focus is that the foreign occupation triggers the secular and religious suicide terrorism much like smoking triggers lung cancer. In Afghanistan before 2001, there were zero suicide attacks in the history of this country. For the first few years, there were some tiny numbers of suicide attacks but in 2006 suddenly there is a spike and it stays high (Graph III). Why?

Looking at the targets of the suicide attacks, majority were the US and Allied troops (73.7%). Over 90% of the suicide attackers were Afghan nationals. A few percent were from the border regions and only 5% were from the regions out of the conflict. But why sudden spike in 2006?

The reason is this. In the first few years, there were only a few thousand US troops in Afghanistan stationed specifically in Kabul, not spread around the country, basically giving security to Karzai, until in 2006, when the UN gave the mandate to the US to spread around Afghanistan. First, the forces went north, where the Northern Alliance were allies with the US, so no problem, then to west, also allies. Then in 2006 the forces moved to South and East (Pashtoon territories), that's when the suicide attacks explode suddenly. The pattern is similar for Pakistan.

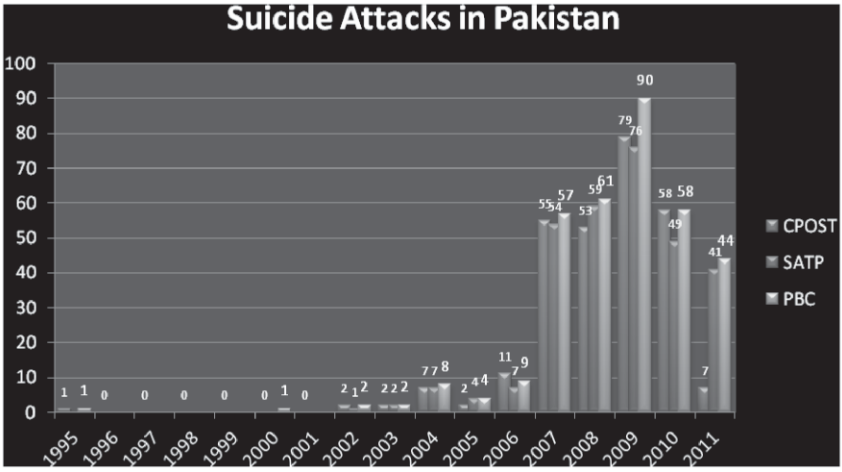
Graph III: Suicide Attacks in Afghanistan (2002 - 2011)



Source:
Chicago Project on Security and Terrorism (CPOST) Database.
Retrieve Jan 30, 2012 from http://cpost.uchicago.edu/search_results.php

According to the Graph III, before the US occupation of Afghanistan, the suicide attacks were very rare in Pakistan (only one case before US occupation). However, as the US attacked Afghanistan, the suicide terrorism started to grew gradually. However, the point is, it didn't grow suddenly after the US invasion. For the first few (5) years, till 2006, the suicide attacks remained relatively lower, both in Pakistan as well as in Afghanistan. However, it mushroomed in 2006-07. In 2006, as mentioned earlier, the US forces moved to East and South of Afghanistan to occupy the Pashtoon territories, at the same time they put pressure on Musharraf (the then President of Pakistan) to withdraw its one hundred thousand (100,000) troops from the Indian border to the Western Pashtoon area. The aim was to indirectly occupy the other half of the Pashtoon area in Pakistan (as the Pashtoon lives on both sides of the Pak-Afghan border). This military presence triggered the suicide terrorism, both in Afghanistan and in Pakistan from 2006 onward.

Graph IV: Trend in Suicide Attacks in Pakistan since 1995



Sources :

(1) Chicago Project on Security and Terrorism (CPOST) Database. Retrieve Jan 30, 2012 from http://cpost.uchicago.edu/search_results.php

(2) Fidayeen (Suicide Squad) Attacks in Pakistan. South Asian Terrorism Portal (SATP). Retrieve Feb10, 2012 from http://www.satp.org/satporgtp/countries/pakistan/database/Fidayeenattack.htm

(3) Pakistan Body Count (PBC). Retrieved Feb 12, 2011 from http://pakistanbodycount.org/suicide_bombing

We find out earlier in Graph IV that KP, FATA and PATA experienced significantly more suicide terrorist attacks than any other part of Pakistan. In Pape's paradigm, it is obvious to conclude that this was a response to the military operations in these areas (predominantly Pashtoon areas).

The major target of these attacks was security forces (57%).[39] The trend is still moving on and the curve didn't go down significantly (Graph III and IV) in both of the countries—Pakistan and Afghanistan. Robert Pape claims that this suicide terrorism is not a Global Jihad but a local opposition to the US and NATO military presence in Afghan territory. The suicide attackers are not just Afghan nationals but Pashtoons from the South and the East in Afghanistan and West in Pakistan (see Table VI for details of suicide attacks in Pakistan).

Table VI: History of Suicide Attacks in Pakistan (1995-2011)

Suicide Attacks in Pakistan												
Year	Attacks			Killed			Wounded			Lethality		
	CPOST*	PCB**	SATP***	CPOST*	PCB**	SATP***	CPOST*	PCB**	SATP***	CPOST*	PCB**	SATP***
1995	1	1	-	17	15	-	60	60	-	17	15	-
1996	-		-	-		-	-		-	-	-	-
1997	-		-	-		-	-		-	-	-	-
1998	-		-	-		-	-		-	-	-	-
1999	-		-	-		-	-		-	-	-	-
2000	-	1	-	-	3	-	-	3	-	-	3	-
2001	-		-	-		-	-		-	-	-	-
2002	2	2	1	26	27	15	76	91	34	13	13.5	15
2003	2	2	2	66	65	69	102	115	103	33	32.5	35
2004	7	8	7	143	82	89	270	399	321	20	10.25	13
2005	2	4	4	24	83	84	80	230	219	12	20.75	21
2006	11	9	7	139	161	161	263	230	352	13	17.888889	23
2007	55	57	54	724	842	765	1315	2008	1677	13	14.77193	14
2008	53	61	59	769	940	893	1729	2426	1846	15	15.409836	15
2009	79	90	76	1038	1090	949	2847	3462	2356	13	12.111111	12

Suicide Attacks in Pakistan

Year	Attacks			Killed			Wounded			Lethality		
	CPOST*	PCB**	SATP***	CPOST*	PCB**	SATP***	CPOST*	PCB**	SATP***	CPOST*	PCB**	SATP***
2010	58	58	49	1160	1153	1167	2775	2954	2199	20	19.87931	24
2011	41	44	41	628	625	628	1183	1386	1183	15	14.204545	15
Total	**311**	**337**	**300**	**4734**	**5086**	**4820**	**10700**	**13364**	**10290**	**15**	**15.09199**	**16**

[1]Source: Chicago Project on Security and Terrorism (CPOST) Database. Retrieve Jan 30, 2012 from http://cpost.uchicago.edu/search_results.php

[2] Pakistan Body Count. Retrieved Feb 12, 2012 from http://pakistanbodycount.org/suicide_bombing

[3]Fidayeen (Suicide Squad) Attacks in Pakistan. South Asian Terrorism Portal (SATP). Retrieve Feb10, 2012 from http://www.satp.org/satporgtp/countries/pakistan/database/Fidayeenattack.htm

**Chicago Project on Security and Terrorism*

*** Pakistan Body Count*

****South Asian Terrorism Portal*

Questions are raised about the confidence in the data which Robert Pape collected through CPOST. However, the data of SATP and Pakistan Body Count (PBC) does not significantly vary from that of CPOST. In Graph IV, the data from CPOST, PBC and SATP are shown side by side. The bars in the Graph do not show any significant variation between the two. It is inferred on the basis of these two independent data sources that the basic motivating factor behind suicide terrorism is not the religion, though religion is used in the national context to fight the unjust and oppressive militaries and their allies, not to bring Sharia or Islamic rule in the land.

Conclusion

Madaris hold a significant position in the Muslim societies and Pakistan is no different. Its influence is deep rooted in Pakistani society, its history and politics. Madaris are a platform to mobilize the masses of Pakistan against or for any cause or force. Though conservative in orientation, the Madaris hold independent thinking and its independence is dear to them. Indeed, reforms are a need of the hour in the Madaris of Pakistan. However, blaming the Madaris for producing suicide terrorist is only a myth created by the Western and Pakistani print and electronic media. The purpose behind which is not still clear. The media need to reconsider its policies of biasness. Media reporting should be on the basis of research.

End Notes

[1]Jessica Stern. (2000). Pakistan's Jihad Culture. In *Foreign Affairs*. 79 no.6 2000; and Jessica Stern. (2001) Meeting with the Muj. In *Bulletin of the Atomic Scientist*. 57 no.1. (Jan-Feb 2001).

[2]Rasheed Khalid. (Monday Feb 15, 2010). "Every Suicide Bomber is Coming from Madrassa". *The News*. Retrieved Feb 3, 2012 from http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=224355&Cat=2&dt=2/15/2010

[3]Jessica Stern. (2000). Pakistan's Jihad Culture. In *Foreign Affairs*. 79 no.6 2000; and Jessica Stern. (2001) Meeting with the Muj. In *Bulletin of the Atomic Scientist*. 57 no.1. (Jan-Feb 2001).

[4]Uzma Anzar. (2003). Islamic Education: A Brief History of Madrassas With Comments on Curricula and Current Pedagogical Practices. Retrieved Feb 2, 2012 from http://www.uvm.edu/~envprog/madrassah/madrassah-history.pdf

[5]Ibid.

[6]Ibid.

[7]Haqqani, Husain, Islam's Medieval Outposts, *Foreign Policy Magazine*, November 2002.

[8]www.Islamicweb.com

[9]Uzma Anzar. (2003). *Opt. Cit.*

[10]History of Religious Madaris. *Monthly* Bainat [Urdu]. Vol.73.No.6. June, 2010. Retrieved Feb 3, 2012 from http://www.banuri.edu.pk/ur/node/1105

[11]Abdul Hasnat Nadvi. (1989). *Hindustan ki Qadeem Darsgahen* [Urdu]. [Old Schools of India]. Lahore: National Book Foundation.p.2.

[12]Ibid

[13]M.Taqi Usmani (1989, 2005). *Our Education System [Hamara Nizam-e-Taleem Kya Hua] Urdu*. Karachi: Maktaba Darul Uloom. pp.71-73

[14]Abdul Hasnat Nadvi. (1989). *Hindustan ki Qadeem Darsgahen* [Urdu]. [Old Schools of India]. Lahore: National Book Foundation.p.2.

[15]Ibid

[16]Taqi Usmani. *Op. Cit*. p.77

[17]Khalid Rehman. (2009). Madrassah in Pakistan: Role and Emerging Trend. In Amit Pandya and Ellew Laipson (eds). *Islam and Politics, Renewal and Resistance in the Muslim World*. Islamabad: Institute of Policy Studies. P.57.

[18]Ibid.

[198]Syed Akhtar Ali Shah. (2011). Role Madrassahs in the Politics of Pakistan. In *Pakistan Journal of Criminology*. Vol.3.No.1.Jan 2011.p.31.

[20]Prakhar Sharma. (2009). Role of Religion in Afghan Politics: Evolution and Key Trends. In In Amit Pandya and Ellew Laipson (eds). *Islam and Politics, Renewal and Resistance in the Muslim World*. Islamabad: Institute of Policy Studies. P. 38.

[21]Syed Akhtar Ali Shah. (2011). The Role of Madrassahs (Islamic Seminaries) in the Politics of Pakistan. *Pakistan Journal of Criminology*. Vol.3.No.1.Jan 2011.pp.9-34.

[22]Ibid

[23]*Pakistan Education Statistics 2007-08*. Academy of Educational Planning and Management, National Educational Management Information System, Ministry of Education, Islamabad, Pakistan; the population estimates are taken from the Wikipedia with different search terms for each of the provinces of Pakistan.

[24]Michael Georgy. (Friday, Feb 11, 2011) *Brainwashing drives young Pakistan suicide bombers*. MARDAN, Pakistan Retrieved, Jan 12, 2012, from http://www.reuters.com/article/2011/02/11/us-pakistan-bombers-youth-feature-idUSTRE71A35I20110211

[25]Rasheed Khalid. (Monday Feb 15, 2010). "Every Suicide Bomber is Coming from Madrassa". *The News*. Retrieved Feb 3, 2012 from http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=224355&Cat=2&dt=2/15/2010

[26]*Pakistan Education Statistics 2007-08*. Academy of Educational Planning and Management, National Educational Management Information System, Ministry of Education, Islamabad, Pakistan; the population estimates are taken from the Wikipedia with different search terms for each of the provinces of Pakistan.

[27]PATA (Provincially Administered Tribal Area) includes Malakand Agency, Swat, Shanglah, Upper-Dir, Lower-Dir, Chitral, and Buner districts of KPK. It is administratively connected with KPK.

[28]Amir Mir. (Sep 13, 2011). Ten years after 9/11: Suicide attacks declining in Pakistan. in *The News*. http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=67436&Cat=6

[29]Holmes S. (2005). Al-Qaeda, September 11, 2001. In Gambetta D, eds. *Making Sense of Suicide Missions*. New York: Oxford University Press.

[30]Saleem Safi. (2009). *Geo News, Exclusive Jirga - Interview with a Suicide Bomber - 2nd July 2009 (Part 1 of 3)*. Retrieved Jan 22, 2012 from http://www.youtube.com/watch?v=nq88egK755k

[31]Ibid

[32]Naushad Ali Khan. (2009). *Op. Cit.*

[33]Saleem Safi. (2009). *Geo News, Exclusive Jirga - Interview with a Suicide Bomber - 2nd July 2009 (Part 3 of 3)* Retrieved Jan 22, 2012 from http://www.youtube.com/watch?v=OeOExvUZHKw&feature=relmfu

[34]Zakir Hassnain. (May 07, 2007). Clerics worried by lack of respect for fatwas on suicide. In *Daily Times*. Retrieved Jan 22, 2012 from http://www.dailytimes.com.pk/default.asp?page=2007%5C05%5C07%5Cstory_7-5-2007_pg7_11

[35]Robert Pape. (2005). *Dying to Win: The Strategic Logic of Suicide Terrorism.* [1st Ed]. New York: Random House.

[36]C.Christine Fair. (2009). *The Madrassah Challenge, Militancy and Religious Education in Pakistan*. Lahore: Vanguard Books. pp. 68-69.

[37]Naushad Ali Khan. (2009). Suicide Bombing in the NWFP: The Need for Research and Information Collection on Human Bombers. In *Pakistan Journal of Criminology*: Vol. 1, Number 1, April, 2009.p.74.

[38]Bombing at Egypt's Embassy in Pakistan Kills 15. (20th November, 1995). *New York Times*. Retrieved, Feb 12, 2011 from http://www.nytimes.com/1995/11/20/world/bombing-at-egypt-s-embassy-in-pakistan-kills-15.html

[39]Chicago Project on Security and Terrorism (CPOST) Database. Retrieve Jan 30, 2012 from http://cpost.uchicago.edu/search_results.php

References

Anzar, U. (2003). Islamic Education: A Brief History of Madrassas With Comments on Curricula and Current Pedagogical Practices. Retrieved Feb 2, 2012 from http://www.uvm.edu/~envprog/madrassah/madrassah-history.pdf

Bombing at Egypt's Embassy in Pakistan Kills 15. (20th November, 1995). New York Times. Retrieved, Feb 12, 2011 from http://www.nytimes.com/1995/11/20/world/bombing-at-egypt-s-embassy-in-pakistan-kills-15.html

Chicago Project on Security and Terrorism (CPOST) Database. Retrieve Jan 30, 2012 from http://cpost.uchicago.edu/search_results.php

Fair, C. Christine. (2009). The Madrassah Challenge, Militancy and Religious Education in Pakistan. Lahore: Vanguard Books.

Georgy, M. (Friday, Feb 11, 2011) Brainwashing drives young Pakistan suicide bombers. MARDAN, Pakistan Retrieved, Jan 12, 2012, from http://www.reuters.com/article/2011/02/11/us-pakistan-bombers-youth-feature-idUSTRE71A35I20110211

Government of Pakistan. (2009). Pakistan Education Statistics 2007-08. Academy of Educational Planning and Management, National Educational Management Information System, Ministry of Education, Islamabad, Pakistan.

Haqqani, H. (2002). Islam's Medieval Outposts. In Foreign Policy Magazine. November 2002.

Hassnain, Z. (May 07, 2007). Clerics worried by lack of respect for fatwas on suicide. In Daily Times. Retrieved Jan 22, 2012 from http://www.dailytimes.com.pk/default.asp?page=2007%5C05%5C07%5Cstory_7-5-2007_pg7_11

History of Religious Madaris. Monthly Bainat [Urdu]. Vol.73.No.6. June, 2010. Retrieved Feb 3, 2012 from http://www.banuri.edu.pk/ur/node/1105

Holmes, S. (2005). Al-Qaeda, September 11, 2001. In Gambetta D, eds. Making Sense of Suicide Missions. New York: Oxford University Press.

Khalid, R. (Monday Feb 15, 2010). “Every Suicide Bomber is Coming from Madrassa”. The News. Retrieved Feb 3, 2012 from http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=224355&Cat=2&dt=2/15/2010

Khan, A. Naushad. (2009). Suicide Bombing in the NWFP: The Need for Research and Information Collection on Human Bombers. In Pakistan Journal of Criminology: Vol. 1, Number 1, April, 2009.

Mir, A. (Sep 13, 2011). Ten years after 9/11: Suicide attacks declining in Pakistan. in The News.

http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=67436&Cat=6

Nadvi, A. Hasan. (1989). Hindustan ki Qadeem Darsgahen [Urdu]. [Old Schools of India]. Lahore: National Book Foundation.

Pape, R. (2005). Dying to Win: The Strategic Logic of Suicide Terrorism. [1st Ed]. New York: Random House.

Rehman, K. (2009). Madrassah in Pakistan: Role and Emerging Trend. In Amit Pandya and Ellew Laipson (eds). Islam and Politics, Renewal and Resistance in the Muslim World. Islamabad: Institute of Policy Studies.

Safi, S. (2009). Geo News, Exclusive Jirga - Interview with a Suicide Bomber - 2nd July 2009 (Part 1 of 3). Retrieved Jan 22, 2012 from http://www.youtube.com/watch?v=nq88egK755k

Saleem Safi. (2009). Geo News, Exclusive Jirga - Interview with a Suicide Bomber - 2nd July 2009 (Part 3 of 3) Retrieved Jan 22, 2012 from http://www.youtube.com/watch?v=OeOExvUZHKw&feature=relmfu

Shah, A. S. (2011). Role Madrassahs in the Politics of Pakistan. In Pakistan Journal of Criminology. Vol.3.No.1.Jan 2011.

Sharma, P. (2009). Role of Religion in Afghan Politics: Evolution and Key Trends. In In Amit Pandya and Ellew Laipson (eds). Islam and Politics, Renewal and Resistance in the Muslim World. Islamabad: Institute of Policy Studies..

Stern, J. (2000). Pakistan's Jihad Culture. In Foreign Affairs. 79 no.6 2000; and Jessica Stern. (2001) Meeting with the Muj. In Bulletin of the Atomic Scientist. 57 no.1. (Jan-Feb 2001).

Usmani, T. Muhammad. (1989, 2005). Our Education System [Hamara Nizam-e-Taleem Kya Hua] Urdu. Karachi: Maktaba Darul Uloom.

The author Fasihuddin (PSP) is a senior police officer in Pakistan. He is also the Editor-in-Chief of Pakistan Journal of Criminology. He can be reached at fasih68@hotmail.com

and The Author Imran Ahmad Sajid is a Gold Medalist in Social Work from University of Peshawar. Currently he is pursuing his Ph.D. Degree from the University of Peshawar. He is the General Secretary of Pakistan Society of Criminology. He can be reached at imranahmad131@gmail.com.

The Dark Side of Social Media: Review of Online Terrorism

Dr. Geoff Dean, Peter Bell, Jack Newman

Abstract

This paper lays the conceptual foundation for understanding the significant role that social media can and does play in relation to spreading the threat and growth of terrorism, especially 'home-grown' terrorism. The utility of social media applications (eg. Facebook, Twitter, You Tube) to recruit, communicate and train terrorists is explored through the perspective of Knowledge-Managed Policing (KMP). The paper concludes with the implications this conceptual analysis of terrorism as a new dot.com presence on the internet has for law enforcement and the global cyber community.

Introduction

The advent of social media (eg. Facebook, Twitter, You Tube) has created new opportunities for terrorist organisations and brought with it growing challenges for law enforcement and intelligence agencies. Whilst the use of online resources by terrorist organisations is not a new occurrence, what is new is the shift to a broader focus by national intelligence agencies towards the increasing threat of 'home-grown' terrorism (ABC News, 2005, 2011; Johnson, 2010; Silber and Bhatt 2007; Wright 2006). A review of extant literature shows a dearth of research into the connection between theoretical and practical applications of social media by terrorist groups and the strategies available to counteract such use.

This study seeks to address aspects of this conceptual gap in the literature by outlining a framework based on a Knowledge-Managed Policing (KMP) approach to the analysis of social media use by terrorists. Three of the most popular social media applications - Facebook, Twitter and YouTube – are focused on in this study as examples of how 'online terrorism' has become a new dot.com with the potential to harness the power of social media for recruiting, communicating, training and funding 'home-grown' terrorists.

Social Media's Utility for Terrorism

The introduction of Web 2.0 applications—websites based solely on interactive user-generated content, or 'social media', as opposed to more traditional static websites where users can only view content (Tech Pluto, 2009; Vorvoreanu and Kisselburgh, 2010) over the last 10 years has created new opportunities for online engagement. These social media sites effectively create online communities based upon users generating, collaborating on, viewing, and sharing content (Tech Pluto, 2009; Vorvoreanu and Kisselburgh, 2010). Wikipedia, as an example, is a free online encyclopaedia that only contains articles generated, edited and reviewed by its user base (Wikipedia, 2011).

The uptake of social media websites by the general public increased rapidly with the emergence of websites such as MySpace and Facebook, which allowed people to 'connect' online with their friends and family, and encouraged the creation of online communities based on common interests, political ideologies or geographical locations (Wooley et al., 2010). As the statistics began to appear showing the incredible surge in popularity of social media websites, people from all political persuasions quickly realised the value of this new resource (Wooley et al., 2010).

Social media quickly presented itself as a cheap and effective tool for mass-communication, as well as an effective method of specifically targeting key demographics (Earl and Kimport, 2011; Papic and Noonan, 2011; Wooley, et al., 2010). As far back as the 1990's political groups and leaders have used the Internet for political purposes (Earl and Kimport, 2011; Wooley et al., 2010). However, this was largely limited to the use of dedicated websites and e-mailing lists to distribute their campaign messages to constituents (Earl and Kimport, 2011).

With the advent of Web 2.0 technology the use of static forms of social media for political use were transformed into more dynamic and ever-evolving phenomena. For instance, in 2008 the value of social media was evidenced during the US Elections with the then presidential candidate, Barack Obama, investing a significant amount of time developing a Facebook page, Twitter account and YouTube channel (Wooley et al., 2010). However, it soon became apparent that social media could be used for other political purposes, from simply providing a forum for like-minded political dissidents to voice their opinions, to being used for organising and instigating major political riots and even revolutions (Earl and Kimport, 2011; Papic and Noonan, 2011).

Three of the most popular social media sites are Facebook, Twitter, and YouTube (Alexa, 2011b). Whilst these applications use different technologies, one important similarity between them is that any person with a valid email address and who claims to be over 13 years old can register as a user on the site (Facebook, 2011; Parental Guide, n.d; Twitter, 2011; YouTube, 2011)—affording a measure of anonymity to users if they require it. Furthermore, it is notable that recently the most popular social media sites have seen an increase in integration, so that content posted on one social media site will simultaneously appear on all other connected sites (Angelos, 2007; Gannes, 2009; Kelsey, 2010; O'Neill, 2009; Swisher, 2008).

Facebook – Virtual Recruitment Strategy

Facebook falls into the 'social networking' category of social media; its primary function is to build and maintain relationships between people (Alexa, 2011a; Wooley et al., 2010). Users of Facebook create an online profile using their personal

details, add connections to friends or family (or strangers, if desired), and can then post 'status updates' on their page or write messages to other users. Members can also create and join 'groups' based on similar interests such as support for a particular political group or cause (Wooley et al., 2010).

In addition to the inherent advantage of being the most widely used social media site throughout the world, the 'groups' application within Facebook presents itself as an invaluable tool for terrorist groups to organise themselves online, and attract other like-minded people to their cause (Wooley et al., 2010). Groups are public by default, and members of the group can send out invitations to friends to recommend that they also join. In this fashion groups can very quickly increase in size, especially when a political purpose is involved (Wooley et al., 2010). Once a group has its user base, any member can send out notifications or messages to every user who has joined the group instantaneously and free of charge (Wooley et al., 2010).

Facebook provides what is essentially an 'all-in-one' service to any group who knows how to use it. While Facebook is certainly capable of acting as a communication service similar to Twitter, and is capable of hosting videos similar to YouTube, the primary function of Facebook for terrorist organisations is for recruitment purposes (Department of Homeland Security, 2010; Torok, 2010). Traditionally, the online presence of a terrorist organisation consisted primarily of a website and possibly a private forum to facilitate jihadist discussions. The problem with this model, as pointed out by a forum poster on a jihadist website, was that an 'elitist community' was created, with those people on the outside having difficulty accessing the community (Department of Homeland Security, 2010). Facebook allows terrorist organisations to avoid this issue.

The most important and useful Facebook feature for terrorist organisations is the 'groups' function (Torok, 2010). The apparent strategy used by terrorist organisations is to create a Facebook group based on a seemingly innocent ideal, such as supporting Palestinians or Islam in general (Department of Homeland Security, 2010; Torok, 2010). As member numbers for the groups increase, jihadist material can be slowly introduced by members of the organisation to the Facebook group in a way which does not directly condone or encourage jihadist actions, and thus does not constitute a violation of Facebook policy (Department of Homeland Security, 2010; Torok, 2010). From this position, the group can even be directed straight to the website and forums of the terrorist organisation behind the Facebook group.

The threat posed by online recruitment is significant (Stein, 2011; al-Shishani, 2010; Weimann, 2010). There are no borders to be crossed, and no effective methods for intervention (Department of Homeland Security, 2010; Torok, 2010). Facebook

allows terrorist organisations to recruit people from all around the world, without posing any significant threat to the security of the organisation (Department of Homeland Security, 2010; Torok, 2010). Importantly, once people become members of the group, the organisation can then seamlessly transition into the next phase: training.

Twitter –Instant Communication Strategy

Twitter falls into the 'blogging' category of social media; however it is more aptly described as a 'micro-blogging' service (Van der Zee, 2009). Registered users of the site post publicly visible messages on their profile called 'tweets': text-based messages of up to 140 characters (Van der Zee, 2009). Users can subscribe to other users to automatically receive their posts, and can follow specific topics by using 'hashtags' (#), which are used to flag posts as belonging to a certain group or topic (Van der Zee, 2009), for example #terrorism to follow tweets related to the topic of 'terrorism'.

The ability to instantaneously send small bits of information to a virtually unlimited number of people free of charge makes Twitter an extremely valuable tool for political purposes (Papic and Noonan, 2011; Van der Zee,2009). Twitter hashtag groups can function in a similar way to Facebook groups, except without a designated leader, with users often 'retweeting' (re-posting) to ensure the message is spread (Van der Zee, 2009). This is in part where the real value of Twitter lies: in the constantly changing virtual communities that are created almost naturally during major events (Papic and Noonan, 2011; Van der Zee, 2009). Political movements and protests in particular see these online communities thrive, where large amounts of people both directly and indirectly involved in an incident begin flocking to follow the relative hashtag for the event (Papic and Noonan, 2011; Van der Zee, 2009).

The threat posed by Twitter arises from both its ability to send out instant messages to large numbers of people, and from the ability for people to follow particular topics as well as groups (O'Rourke, 2010). Terrorist organisations can utilise Twitter at an operation level, using the service to keep up-to-date on any new information that emerges in the public sphere (Weimann, 2010; O'Rourke, 2010; US 304th Military Intelligence battalion, 2008). The 2008 terrorist attacks in Mumbai present an apt example of how terrorist organisations can utilise social media sites such as Twitter.

The 2008 Mumbai terrorist attacks occurred on 26 November, with more than 10 sites throughout Mumbai targeted by an Islamic terrorist organisation from Pakistan: Lashkar-e-Taiba (O'Rourke, 2010). The attacks killed 164 people and injured over 300. One of the most important issues that arose from the attacks was

the technological sophistication of the attackers. All of the attackers were equipped with BlackBerry smart-phones, and not only utilised VOIP (Voice over Internet Protocol), but also carried multiple SIM cards to switch into the phones if authorities were able to block them (O'Rourke, 2010; US 304th Military Intelligence battalion, 2008).

Post-attack interviews with the sole surviving attacker, combined with information from intercepted phone calls from the attackers during the events indicated that the terrorists were in constant contact with controllers based in Pakistan (O'Rourke, 2010; Rabasa et al., 2009). The controllers were able to keep track of the constant up-to-date flow of information streaming from public Twitter posts and communicate it directly to the attackers (Leggio, 2008; O'Rourke, 2010; Rabasa et al., 2009). This included critical information such as the movements and positioning of the Indian counter-terrorism units planning the assault on the hotel (Lee, 2008; Leggio, 2008; O'Rourke, 2010).

Examples such as Mumbai serve to demonstrate the increasingly advanced technological sophistication of terrorist organisations. In order to effectively combat these groups, robust counter-strategies for social media must be developed and implemented by government agencies as soon as possible.

YouTube – Cyber Training Strategy

YouTube falls into the 'video sharing' category of social media; the primary function of the website is to host videos uploaded by users, which are then publicly viewed and shared around the world (Vergani and Zuev, 2011). Registered users of YouTube are able to upload videos in a wide range of formats up to 15 minutes in length, and in most cases viewers do not need to register (Vergani and Zuev, 2011). Registered members can subscribe to another user's YouTube 'channel', receiving alerts whenever a new video is posted on that channel (Vergani and Zuev, 2011). While there are a range of restrictions over what cannot be uploaded, the 'post-hoc' review system used for YouTube videos means that only those videos which have been 'reported' by viewers will be reviewed and potentially removed by YouTube staff, thus making abuse of the system possible by terrorist groups.

YouTube is free, easy to use, difficult for state authorities to control, and can be used to communicate with a tightly-knit group to the entire world (Vergani and Zuev, 2011). Furthermore, YouTube can provide a more effective means of communication than text-based social media sites such as Facebook and Twitter, simply due to the ability to use sound and video (Vergani and Zuev, 2011).

Like Facebook, YouTube has multiple uses for terrorist organisations (Weimann, 2010; Bergin et al, 2009; George, 2009). Video can be a much more effective means of communicating an issue than plain text, so for this reason alone

YouTube would be an invaluable tool for terrorist organisations (Torok, 2010). For example, Anwar Al Awlaki is a prominent and 'highly dangerous' planner and trainer for 'Al Qaeda and all of its franchises', well known for his utilisation of social media sites such as Facebook and YouTube to spread his extremist messages (Madhani, 2010; Shephard, 2009; Smith, 2009). As of 2010, Awlaki was known to have posted over 5000 videos on YouTube (Torok, 2010). However, more important than simply relaying a message or calling for people to take action is showing them physically how to do it; this is where YouTube's value for terrorist organisations is truly shown (Department of Homeland Security, 2010).

Videos explaining and visually demonstrating practices such as tactical shooting or the field stripping of an AK47 have been identified as examples of training that is effectively communicated over YouTube (Department of Homeland Security, 2010). Additionally, these types of training videos do not actively incite violence, and thus do not contravene YouTube's policy, and will therefore not be deleted (Department of Homeland Security, 2010). Terrorist organisations can also take advantage of YouTube's 'post-hoc' review system by uploading bomb making instructions and other such videos that violate YouTube policy, but which can potentially be viewed hundreds of times before the videos are reported and deleted.

Terrorism: A New Dot.Com

According to Awan (2010) the internet has surpassed all other media forms in becoming the principle arena for terrorist media activity, and the primary platform for the dissemination of jihadism. Furthermore, this review has demonstrated it is not only political activists who see the competitive advantage of using social media, as the three most popular social media sites (Facebook, Twitter, and YouTube) have value-added to terrorism's ability to communicate, organise, recruit, and train would be terrorists (Alexa, 2011b; Weimann, 2006; Wright, 2006). Furthermore, terrorist groups are also using social media for fundraising purposes (Strohm, 2011; Gray, 2009; Caldwell, 2008; Conway, 2006).

This cluster of issues is of particular relevance to countries like Pakistan with large Muslim populations where fertile minds exist for social media to radicalism free of charge. Moreover, countries such as Australia face their own concerns about social media, where the traditional transnational terrorism threat is being replaced by a much more pervasive and difficult to detect 'home-grown' or 'grass-roots' terrorism threat embedded in virtual realities (Johnson, 2010; ABC News, 2005, 2011; Silber and Bhatt, 2007; Wright, 2006).

This review found that whilst the quality of the literature that focused on terrorists' use of social media was generally of a higher quality than that related to political activism in general, the number of articles available on this issue was

limited (Bjelopera and Randol, 2010; Hoffman, 2010; Silber and Bhatt, 2007; Weimann, 2006). Furthermore, many of the articles had been written by, or for, the US military (Mayfield, 2011; McCullar, 2010; Petraeus, 2010; US Joint Forces Command – Joint Warfighting Center, 2010). While the majority of content in these articles was highly relevant, the recommendations presented for strategies to deal with the issues were focused on military applications, as opposed to more generally applicable strategies or those which were specific to government or intelligence agencies.

Those articles which did not focus on military applications debated the effectiveness of the three broad policy approaches that governments can adopt: zero tolerance, encouraging extremist narrative to be challenged through the same social media tools that promote it, and intelligence gathering (Bergin et al, 2009; Caldwell, 2008).

Hence, what is also clear from this review is that governments, law enforcement and intelligence agencies are adapting to this new political and social environment created by Web 2.0 inspired social media and are seeking to find and adopt new policies and strategies to minimize these threats and harness the presented opportunities. For instance, in June 2011, the Joint Select Committee on Cyber-Safety instituted by the Australian Parliament tabled its report on its Inquiry into Cyber-Safety entitled *High-Wire Act: Cyber-Safety and the Young.*

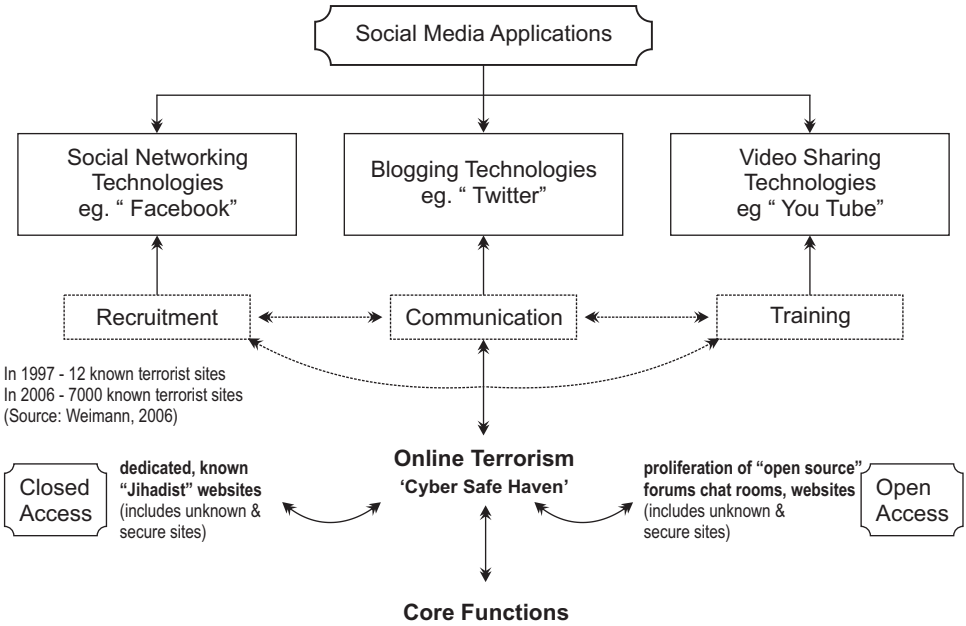
Moreover, there was a rapid expansion and widespread growth of 'Jihadist' websites during the period when Web 2.0 technologies began widely available around 2004 onwards. For instance, research by Weimann (2006) into the use of the Internet by terrorist groups showed that between 1997 and 2006, the number of websites dedicated to terrorist groups rose from only about 12, to over 7000.

Similarly, Stein (2011:3) cites a U.S. State Department report in 1998, that "… there were only 15 Web Sites run by groups defined by US as "terrorist" groups. In 2005, this number increased to more than 4000."

While the terrorist organisations that are advanced enough to have a presence online would traditionally stick to the use of 'jihadist websites' and forums, where most of the users were people already supporting the cause (Department of Homeland Security, 2010), the transition into the more 'open' realm of social media has given them the opportunity to reach significantly larger audiences than was previously possible. For instance, Cohen (2009) found that terrorist groups actively target the large number of social media users among vulnerable populations in impoverished regions in the Middle East, Africa and Asia, and poorly integrated immigrant communities in Western Europe.

Therefore, the conceptual picture which emerges from this review is that Web 2.0 social media technologies have allowed terrorism to become a massive 'dot.com' presence on the internet. Figure 1 below illustrates the virtual pathways utilised by terrorism to carry out its core functions 'online'.

Conceptual Map of Web 2.0 Technologies for Online Terrorism



Information provision (eg. the 3 P's - Publicity, Propaganda, Psychological warfare, including disinformation)
Information gathering (eg. 'data mining' for specific targeting opportunities, intelligence & information sharing)
Networking (eg. decentralized structures, planning & coordination operations, risk mitigation via virtual communities)
Financing (eg. soliciting funds via Jihadist Websites, exploiting e-commerce tools, business, charities, fronts)
Recruitment (eg. recruiting and mobilising followers, sympathizers)

Source: Gray and Head, 2009; Kohlmann, 2008; Conway, 2006;Weimann, 2004

Therefore, the conceptual picture which emerges from this review is that Web 2.0 social media technologies have allowed terrorism to become a massive 'dot.com' presence on the internet. Figure 1 below illustrates the virtual pathways utilised by terrorism to carry out its core functions 'online'.

As can be seen from Figure 1, the conceptual mapping above depicts the phenomenal rise of Jihadist expansion on the web through both closed and open access portals as well as the various configurations of online terrorism. As such, it provides a useful starting point for research but much more work needs to be done before a clearer picture of radicalism and its effectiveness comes into focus.

This is in part due to the very limited amount of scholarly empirical research in the existing literature on the effectiveness of social media by terrorist organisations to radicalise people (Leuprecht and Skillicorn, 2011). Much is anecdotal and based on biased samples. For instance, al-Shishani (2010) reports that "… according to Pakistani authorities, the five young American Muslims arrested in Pakistan last December were recruited online via You Tube and Facebook after the suspects used these sites to reach out to groups such as Lashkar-e-Taiba and Lashkar-e-Jhangyi (*Dawn* [Karachi], December 16)". In addition, there are major issues with the range of quality found in the literature, as well as with the lack of connections made between theory and practical application.

Given such limitations the role of Knowledge Management (KM) in capturing relevant and reliable data, information, intelligence and evidence on which to base policing and law enforcement of social media is still in its infancy. However, KM does have substantial applicability for policing online terrorism. For instance, the notion of 'Knowledge-Managed Policing' (KMP) coined by Dean is a foundational framework for managing, systematically, the application of knowledge to enhance policing effectiveness through harnessing practitioner-based knowledge and integrating such tacit knowledge with KM processes and appropriate IT support systems (Dean and Gottschalk, 2007). Furthermore, the utility of KMP for managing the challenges associated social media must, of necessity, involved a range of Communication Interception Technologies (CIT) by police and other law enforcement agencies. Dean, Bell, and Congram (2010) have previously outlined the significance of KMP as an organising framework for using CIT as an investigative tool for knowledge creation, capture, storage, retrieval, transfer, sharing, application and integration. Moreover, Dean (2007) developed a multi-context model of the terrorism process which is the subject of future work to integrate KMP with this terrorism model in order to expand available counter-terrorism options to police and law enforcement agencies, especially in relation to this dark side of social media.

A special report on *Countering internet radicalisation in Southeast Asia* in 2009 by Bergin, Osman, Ungerer, and Yasin identified three broad policy approaches and/or a combination of them which governments tend to adopt towards dealing with online terrorism. There are as stated in the report (2009:12):

- a hard strategy of *zero tolerance* (blocking sites, prosecuting site administrators, using internet filters)
- a softer strategy of *encouraging internet end users to directly challenge the extremist narrative* (including creating websites to promote tolerance)

- an intelligence-led strategy of *monitoring leading to targeting, investigation, disruption and arrest*.

Essentially, these policy approaches translate into a policing/law enforcement counter-terrorism continuum ranging from prevention to utilisation methodologies.

Prevention Methodologies would include aspects of a '*zero tolerance strategy*' whereby sites are censored, blocked or cut off and aspects of an '*intelligence-led strategy*' of monitoring, targeting, investigating, disrupting and ultimately arresting and prosecuting those involved in terrorist activities. For instance:

- censoring sites, eg. South Korea deletes political content from various social media sites regarded as North Korean propaganda (Eun-jung, 2011)
- blocking sites, eg. 'The Great Firewall of China' where access to websites deemed to be politically sensitive or offensive are blocked (Petraeus, 2010).
- cutting off complete access to the internet for entire regions or countries, eg. during the 2011 revolution in Egypt (Papic and Noonan, 2011)
- Proactive Intelligence monitoring and collection eg. developing risk profiles of potential terrorists through monitoring terrorist-related social media sites, (Norris, 2011)

Utilisation Methodologies would include some aspects of an '*intelligence-led strategy*', mainly that of disinformation, and a softer strategy of *encouraging and challenging extremist narratives.* For instance:

- Disinformation via 'sock puppets', eg. Sock puppets have been used to infiltrate online-based political or terrorist groups, and once inside to spread disinformation about the location and activities of law enforcement to disrupt the plans of the group and/or direct their protest towards a location that can be easily controlled (Norris, 2011; Papic and Noonan, 2011)
- Insider Knowledge' intelligence gathering, eg. tips offs by informers and human assets inside terrorist's cells and sites in order to utilise such knowledge strategically (Norris, 2011)
- Creating alternative websites by moderate Muslim groups, eg. harnessing soical media to promote peace and democracy (Caldwell, 2008); providing alternatives to extremist influence (Cohen, 2009)

All counter-terrorism policy approaches and law enforcement strategic methodologies are depend on and require a substantive investment in a range of resources to counter social media-based radicalisation. The Special report by Bergin et al (2009:13) outlines in broad terms the *technical, human* and *intellectual* resources necessary to deal with online terrorism as follows:

- ***Technical infrastructure***

  The technical requirements are secure, unattributable, superfast (broadband and wireless) ICT systems, and the ability to access and view extremist sites (visibility of the environment is fundamental).

- ***Human resources***

  People with analytical, linguistic and technical skills are essential. They will need adequate training and the support of experts.

- ***Knowledge and intellectual capital***

  It's necessary to stay abreast of the latest trends and industry developments, and governments aren't normally at the forefront of internet-related trends.

This massive investment is ultimately about Knowledge Management and the mobilisation of relevant resources. Since 9/11 and the extraordinary growth of online terrorism, the academic community is also playing a significant role with the emergence of a new interdisciplinary field of study and research known as 'Terrorism informatics' (Chen, Reid, Sinai, Silke, and Ganor, 2008).

According to Chen (2011:1) “Terrorism informatics has been defined as the application of advanced methodologies, information fusion and analysis techniques to acquire, integrate process, analyze, and manage the diversity of terrorism-related information for international and homeland security-related applications.”

Chen notes the wide variety of methods used in 'terrorism informatics' to collect massive amounts of many and varied types of multi-lingual information from multiple sources. Hence, 'terrorism informatics' draws on a diversity of disciplines from Computer Science, Informatics, Statistics, Mathematics, Linguistics, Social Sciences, and Public Policy and their related sub-disciplines to achieve “ Information fusion and information technology analysis techniques, which include data mining, data integration, language translation technologies, and image and video processing, play central roles in the prevention, detection, and remediation of terrorism.” (op. cit).

Conclusion

This review of the extant literature from military, academic and public open sources presents a disturbing picture of the multiple pathways Web 2.0 'social media' technologies provide for terrorists and militant extremists to utilise and develop cyber terrorism into a potent virtual battleground which police and security agencies must confront on a very uneven global playing field.

Furthermore, it is evident from this review that the concept and practice of 'Knowledge-Managed Policing' (KMP) is highly relevant, timely and necessary perspective for policing/law enforcement/security agencies. Adopting a salient Knowledge Management approach can tip the competitive advantage towards policing the multitude of harms and threats that 'online terrorism' presents through the medium of the dark side of social media for Civil Society.

References

ABC News. 2005. ASIO warns of home-grown terror threat. Available from: http://www.abc.net.au/news/stories/2005/11/02/1495641.htm [accessed 04.15.11].

ABC News. 2011. "ASIO sets up cyber-spook unit." Accessed April 16, 2011. Available from: http://www.abc.net.au/news/stories/2011/03/11/3161101.htm

Alexa. 2011a. Facebook.com Site Info. Available from: http://www.alexa.com/siteinfo/facebook.com [accessed 04.04.11].

Alexa. 2011b. Top 500 sites on the web. Available from: http://www.alexa.com/topsites [accessed 04.25.11].

al-Shishani, Murad Batal. 2010. Taking al-Qaeda's Jihad to Facebook. *The Jamestown Foundation: Terrorism Monitor*. 8 (5): 3. Available from: http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=36002 [accessed 08.04.11].

Awan, Akil N. 2010. The Virtual Jihad: An Increasingly Legitimate Form of Warfare. http://www.ctc.usma.edu/posts/the-virtual-jihad-an-increasingly-legitimate-form-of-warfare [accessed 08.04. 2011].

Angelos, A. 2007. Twitter updates now connected to Facebook status. Available from: http://mashable.com/2007/09/30/facebook-Twitter-2/ [accessed 03.30.11].

Barat, J. 2009. Internet Blocked in Uyghur Autonomous Region. Available from: http://www.uighur.nl/Internet-blocked-in-uyghur-autonomous-region/ [accessed 05.05.11].

BBC. 2010. Israeli military 'unfriends' soldier after Facebook leak. Available from: http://news.bbc.co.uk/2/hi/middle_east/8549099.stm [accessed 04.29.11].

Bergin, Anthony; Osman, Sulastri; Ungerer, Carl; Yasin, Nur Auzlin Mohamed. 2009. Countering internet radicalisation in Southeast Asia. *Australian Strategic Policy Institute, Canberra*. Available from: http://www.aspi.org.au/publications/publication_details.aspx?ContentID=202&pubtype=10 [accessed 08.03.11].

Bishop, B. 2010. China's Internet: The Invisible Birdcage. Available from: http://digicha.com/?p=1490 [accessed 05.04.11].

Bjelopera, J., Mark, R. 2010. American Jihadist Terrorism: Combating a Complex Threat. Available from: http://www.fas.org/sgp/crs/terror/R41416.pdf [accessed 05.02.11].

Bray, H. 2009. Finding a way around Iranian censorship. Available from: http://www.boston.com/business/technology/articles/2009/06/19/activists_utilizing_Twitter_web_proxies_to_sidestep_iranian_censorship/?page=2 [accessed 05.01.11].

Bristow, M. 2008. China's Internet 'spin doctors'. Available from: http://news.bbc.co.uk/2/hi/asia-pacific/7783640.stm [accessed 05.07.11].

Chen, Hsinchun; Zhou, Yilu; Reid, Edna F. and Larson, Catherine A. 2011. *Introduction to special issue on terrorism informatics. Information systems frontiers.* 13 (1): 1-3. Available from http://www.springerlink.com.ezp01.library.qut.edu.au/content/p373485141036393/ [accessed 08.01.11].

Chen, H., Reid, E., Sinai, J., Silke, A., & Ganor, B. (Eds.) (2008). Preface. *Terrorism informatics: Knowledge management and data mining for homeland security* (Integrated Series in Information Systems). New York: Springer.

Caldwell, Ingrid. 2008. Terror on YouTube. *Forensic Examiner.* (17)3: 80-83. Availablefrom:http://search.proquest.com.ezp01.library.qut.edu.au/docview/207654544/fulltextPDF/130EDDFAE4C5ACB3E4A/1?accountid=13380 [accessed 08.01.11].

Clayton, R., Murdoch, S., Watson, R. 2006. Ignoring the Great Firewall of China. Available from: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf [accessed 05.03.11].

Cohen, J. 2009. Diverting the Radicalization Track. *Policy Review*. 154: 51-63. Available from: http://search.proquest.com.ezp01.library.qut.edu.au/docview/216455875/fulltextPDF/130F2EF9BC860766293/1?accountid=13380 [accessed 08.03.11].

Conway, Maura. 2006. Terrorism and the Internet: New Media- New Threat? *Parliamentary Affairs.* 59(2): 283-98. Available from: http://pa.oxfordjournals.org.ezp01.library.qut.edu.au/content/59/2/283.full.pdf+html [accessed 08.01.11].

Crampton, T. 2010. Infographic of Social Media Equivalents in China. Available from: http://www.thomascrampton.com/china/social-media-china/ [accessed 05.04.11].

Crampton, T. 2011. China social networks: cool girls to hipsters. Available from:http://www.thomascrampton.com/china/renren-china/ [accessed 05.04.11].

Cyber-Safety Inquiry Report, *High-Wire Act: Cyber-Safety and the Young.* 2011. A Joint Select Committee on Cyber-Safety tabled its report on Monday 20 June 2011 for the Australian Government. Available from: http://www.aph.gov.au/house/committee/jscc/report.htm [accessed 27.06.11].

Dean, G., Bell, P., and Congram, M. 2010. Knowledge-Managed Policing Framework for Communication Interception Technologies (CIT) in Criminal Justice System. *Pakistan Journal of Criminology*, 2 (4) pp.25-41

Dean, G. 2007. Criminal Profiling in a Terrorism Context. In Kocsis, R. (Ed) *Criminal Profiling: International perspectives in theory, practice & research.* Humana Press.

Dean, G. and Gottschalk, P. 2007. *Knowledge Management in Policing and Law Enforcement: Foundations, Structures, Applications.* Oxford University Press: UK.

Department of Homeland Security. 2010. Terrorist use of Social Networking Sites: Facebook Case Study. Available from: http://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/ [accessed 04.20.11].

Earl, J., Kimport, K. 2011. *Digitally Enabled Social Change: Activism in the Internet Age*, Massachusetts Institute of Technology Publishing.

Eun-jung, K. 2011. S. Korean man indicted for pro-Pyongyang postings on Internet, Twitter. Available from: http://english.yonhapnews.co.kr/news/2011/01/10/36/0200000000AEN20110110007200315F.HTML [accessed 05.05.11].

Facebook. 2011. What is the minimum age required to sign up for Facebook? Available from: http://www.facebook.com/help/?page=173#!/help/?faq=13455 [accessed 04.10.11].

Fielding, N. Cobain, I. 2011. Revealed: US spy operation that manipulates social media. Available from: http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks?INTCMP=SRCH [accessed 05.05.11].

Gannes, L. 2009. YouTube integrates Facebook Connect. Available from: http://gigaom.com/video/youtube-integrates-facebook-connect/ [accessed 04.05.11].

Gray, David H. and Head, Albon. 2009. The Importance of the Internet to the Post-Modern Terrorist and its Role as a Form of Safe Haven. *European Journal of Scientific Research.* 25 (3): 396-404. Available from: http://www.eurojournals.com/ejsr_25_3_05.pdf [accessed 08.03.11].

Hennock, M. 2009. The Uighur riots in western China are teaching the government how to spin. Available from: http://www.newsweek.com/2009/07/06/bad-press.html [accessed 05.05.11].

Hoffman, B. 2010. Internet terror recruitment and tradecraft: how can we address an evolving tool while protecting free speech? Available from: http://www.homelandsecurity.house.gov/SiteDocuments/20100526101502-95237.pdf [accessed 04.25.11].

Johnson, T. 2010. Threat of Homegrown Islamist Terrorism. Available from: http://www.cfr.org/terrorism/threat-homegrown-islamist-terrorism/p11509 [accessed 04.20.11].

Kelsey, T. 2010. *Social Networking Spaces: From Facebook to Twitter and Everything In Between*, New York: Springer-Verlag.

Kohlmann, Evan F. 2008. Homegrown Terrorists: Theory and Cases in the War on Terror's Newest Front. *The Annals of the American Academy of Political and Social Science. 618(1): 95-109.* Available from: http://ann.sagepub.com.ezp01.library.qut.edu.au/content/618/1/95.full.pdf+html [accessed 08.03.11].

Lee, M. 2008. Blogs feed information frenzy on Mumbai blasts. Available from: http://www.theglobeandmail.com/news/technology/article725225.ece [accessed 04.17.11].

Leggio, J. 2008. Mumbai attack coverage demonstrates (good and bad) maturation point of social media. Available from: http://www.zdnet.com/blog/feeds/mumbai-attack-coverage-demonstrates-good-and-bad-maturation-point-of-social-media/339 [accessed 04.17.11].

Leuprecht. C., and Skillicorn, D. B. 2011. Radicalisation: What (If Anything) is to be Done? When Facts Get in the Way of a Good Story. *Home Team Journal*, Issue 3 pp. 38-46.

Macleod, Hugh. 2011. Syria's young cyber activists keep protests in view. Available from: http://www.guardian.co.uk/world/2011/apr/15/syria-activists-protests-in-view [accessed 04.12.11].

Madhani, A. 2010. Cleric al-Awlaki dubbed 'bin Laden of the Internet'. Available from: http://www.usatoday.com/news/nation/2010-08-25-1A_Awlaki25_CV_N.htm [accessed 04.15.11].

Malkin, B. 2010. Google refuses Australian government request to censor YouTube. Available from: http://www.telegraph.co.uk/technology/google/7212902/Google-refuses-Australian-government-request-to-censor-YouTube.html [accessed 05.04.11].

Mayfield, T. 2011. A Commander's Strategy for Social Media. Available from:http://www.ndu.edu/press/commanders-strategy-social-media.html [accessed 05.01.11].

McCullar, T. 2010. Information Warfare, Media, and Decisiveness in Counterinsurgency. Information Operations Journal. 2(4), 4-7. Available from: http://www.nxtbook.com/nxtbooks/naylor/JEDQ0410/#/0 [accessed 05.03.11].

Merriam Webster. 2011. Sock Puppet. Available from: [accessed 05.15.11].

Michael, George. 2009. Adam Gadahn and Al-Qaeda's Internet Strategy. *Middle East Policy.* 16 (3): 135-152. Available from: http://onlinelibrary.wiley.com.ezp01.library.qut.edu.au/doi/10.1111/j.1475-4967.2009.00409.x/pdf [accessed 08.04.11].

Mi-ju, K. 2010. Pro-North Facebook entries face gov't crackdown. Available from: http://joongangdaily.joins.com/article/view.asp?aid=2929934 [accessed 05.02.11].

Molok, N., Chang, S., Ahmad, A. 2010. Information Leakage through Online Social networking: Opening the Doorway for Advanced Persistence Threats. Available from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1092&context=ism&sei-redir=1 [accessed 05.02.11].

Norris, J. 2011. UK police using Twitter to track protesters. Available from: http://unplugged.rcrwireless.com/index.php/20110210/news/6955/uk-police-using-Twitter-to-track-protesters/ [accessed 05.07.11].

O'Neill, N. 2009. YouTube adds Facebook Connect. Available from: http://www.allfacebook.com/youtube-adds-facebook-connect-2009-06 [accessed 04.05.11].

OpenNet Initiative. 2009. Internet Filtering in China. Available from: http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf [accessed 05.03.11].

OpenNet Initiative. n.d. Social Media Filtering Map. Available from: http://opennet.net/research/map/socialmedia [accessed 05.15.11].

O'Rourke, S. 2010. The Emergent Challenges for Policing Terrorism: Lessons from Mumbai. Available from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1004&context=act [accessed 04.10.11].

Papic, M. Noonan, S. 2011. Social Media as Tool for Protest. Last modified February 3, 2011. Available from: http://www.stratfor.com/weekly/20110202-social-media-tool-protest?utm_source=SWeekly&utm_medium=email&utm_campaign=110203&utm_content=readmore&elq=77ffb64cf0554757abe76e998eb0395b [accessed 09.07.11].

Parental Guide. n.d. Parents Lying to Gain Online Access for Their Kids on Facebook, Twitter, and MySpace. Available from: http://www.parentalguide.org/parentalcontrols_age-requirements-for-facebook-Twitter-myspace.html [accessed 04.11.11].

Petraeus, D. 2010. The Posture of U.S. Central Command. Available from: [accessed 05.05.11].

Rabasa, A., Blackwill, R., Chalk, P., Cragin, K., Fair, C., Jackson, B., Jenkins, B., Jones, S., Shestak, N., Tellis, A. 2009. The Lessons of Mumbai. Available from: http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf [accessed 04.20.11].

Sanchez, R. 2010. Growing number of prosecutions for videotaping the police. Available from: http://abcnews.go.com/US/TheLaw/videotaping-cops-arrest/story?id=11179076&page=1 [accessed 04.13.11].

Schneier, B. 2008. Internet censorship. Available from: http://www.schneier.com/blog/archives/2008/04/Internet_censor.html [accessed 05.03.11].

Shephard, M. 2009. The powerful online voice of jihad. Available from: http://www.thestar.com/news/world/article/711964--the-powerful-online-voice-of-jihad [accessed 04.15.11].

Silber, M. Bhatt, A. 2007. Radicalization in the West: The Homegrown Threat. Available from:http://sethgodin.typepad.com/seths_blog/files/NYPD_Report-Radicalization_in_the_West.pdf [accessed 04.20.11].

Smith, H. 2009. Al-Awlaki May Be Al-Qaeda Recruiter. Available from: http://www.cbsnews.com/8301-503543_162-6039811-503543.html [accessed 04.12.11].

Stein, Yael. 2011. Social Networks – Terrorism's New Marketplace. *Genocide Prevention Now.* Available from: http://www.genocidepreventionnow.org/Portals/0/docs/Al%20Quaeda%20is%20recruiting%20on%20Facebook.pdf [accessed 08.04.11].

Stone, B. Richtel, M. 2007. The Hand That Controls the Sock Puppet Could Get Slapped. Available from: http://www.nytimes.com/2007/07/16/technology/16blog.html?ex=1342238400&en=9a3424961f9d2163&ei=5088&partner=rssnyt&emc=rss [accessed 05.10.11].

Strohm, Chris. 2011. Facebook, YouTube Aid in Al-Qaida's Spread, Study Says. *National Journal.* Available from: http://search.proquest.com.ezp01.library.qut.edu.au/docview/850518421# [accessed 08.02.11].

Swisher, K. 2008. When Twitter Met Facebook: The Acquisition Deal That Fail-Whaled. Available from: http://kara.allthingsd.com/20081124/when-Twitter-met-facebook-the-acquisition-deal-that-fail-whaled/ [accessed 03.30.11].

Tech Pluto. 2009. Core Characteristics of Web 2.0 Services. Accessed April 5, 2011. Available from: http://www.techpluto.com/web-20-services/ [accessed 04.05.11].

Torok, R. 2010. 'Make a Bomb In Your Mum's Kitchen': Cyber Recruiting And Socialisation of 'White Moors' and Home Grown Jihadists. Available from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1005&context=act [accessed 04.20.11].

Twitter. 2011. Twitter Privacy Policy. Available from: https://Twitter.com/privacy [accessed 04.10.11].

US 304th Military Intelligence Battalion. 2008. Sample Overview: alQaida-Like Mobile Discussions & Potential Creative Uses. Available from: http://www.fas.org/irp/eprint/mobile.pdf [accessed 04.28.11].

US Joint Forces Command – Joint Warfighting Center. 2010. Commander's Handbook for Strategic Communication and Communication Strategy. Available from: [accessed 05.07.11].

Van der Zee, B. 2009. Twitter Triumphs. Index on Censorship. 38(4), 97-102. Doi: 10.1080/03064220903392570 [accessed 04.20.11].

Vergani, M. Zuev, D. 2011. Analysis of YouTube Videos Used by Activists in the Uyghur Nationalist Movement: combining quantitative and qualitative methods. *Journal of Contemporary China*. 20(69), 205-229. Doi: 10.1080/10670564.2011.541628

Vorvoreanu, M. Kisselburgh, L. 2010. Web 2.0: A Complex Balancing Act. Available from: http://www.mcafee.com/us/resources/reports/rp-first-global-study-web-2.0-usage.pdf [accessed 04.10.11].

Weimann, G. 2010. Terror on Facebook, Twitter, and Youtube. *The Brown Journal of World Affairs*. 16 (2): 45-54. Available from: http://search.proquest.com.ezp01.library.qut.edu.au/docview/347853609/fulltextPDF/130DF8DC3A413223544/2?accountid=13380 [accessed 07.29.11].

Weimann, G. 2006. *Terror on the Internet: the New Arena, the New Challenges*. Washington, DC: United States Institute of Peace Press.

Wikipedia. 2011. Wikipedia: About. Last modified April 7, 2011. Available from:

http://en.wikipedia.org/wiki/Wikipedia:About [accessed 15.10.11].

Wikipedia. 2011. Web 2.0. Last modified April 7, 2011. Available from:

http://en.wikipedia.org/wiki/Wikipedia:About [accessed 05.10.11].

Williams, M. 2010. South Korea has begun blocking access to a Twitter account operated by a North Korean Web site. Available from: http://www.reuters.com/article/2010/08/20/urnidgns852573c40069388000257785000b-idUS56724690620100820 [accessed 05.02.11].

Woolley, J.K., Limperos, A.M. Beth, M. 2010. The 2008 Presidential Election,

2.0: A Content Analysis of User-Generated Political Facebook Groups. *Mass Communication and Society.* 13(5), 631-652. Doi:10.1080/15205436.2010.516864 [accessed 03.20.11].

Wright, L. 2006. ASIO scans Muslim web surfers. Available from: http://www.news.com.au/national/asio-scans-muslim-web-surfers/story-e6frfkx0-1111112257310 [accessed 04.14.11].

Wright, R. 2009. In Iran, One Woman's Death May Have Many Consequences. Available from: http://www.time.com/time/world/article/0,8599,1906049,00.html [accessed 04.20.11].

Wtwu. 2011. Hints and Tips for Whistleblowers. Available from: https://p10.secure.hostingprod.com/@spyblog.org.uk/ssl/ht4w/index.html [accessed 04.25.11].

YouTube. 2011. Teenage Safety. Available from: http://www.google.com/support/youtube/bin/answer.py?hl=en-GB&answer=126262 [accessed 04.11.11].

The author *Dr. Geoff Dean* is Associate Professor in the School of Justice in the Faculty of Law at the Queensland University of Technology in Brisbane, Australia. His current areas of expertise, teaching specialisation and research are in Knowledge-Managed Policing, the cognitive psychology of investigative thinking, criminal and terrorism profiling, global organised crime and international policing. Dr. Dean has extensive publications in international journals and is the principal author of the book *Knowledge Management in Policing and Law Enforcement: Foundations, Structures, Applications* published by Oxford University Press in the UK in 2007. Dr. Dean was principal Guest Editor of a Special Issue on 'Local Research Links to Global Policing' in *Police Practice and Research: An International Journal*, Vol 9, No.4 in 2008. His latest book as principal author is *Organised Crime: Policing Illegal Business Entrepreneurialism* published in UK in 2010 by Oxford University Press.

The author *Dr. Peter Bell* is a Senior Lecturer and the Director of Postgraduate Studies at the School of Justice in the Faculty of Law. He has wide and diverse experience in policing, law enforcement and security including senior analytical and operational positions with the Queensland Police Service, the Australian Bureau of Criminal Intelligence, the Australian Federal Police and the Organised Crime Agency of British Columbia- Canada (OCABC). Dr Bell has written extensively for police/security agencies on topics to do with official corruption, international drug trafficking, terrorism, critical infrastructure security and transnational organised crime.

And the author *Jack Newman* holds a Bachelor of Justice majoring in Policing and Criminology, and Graduate Certificate in Intelligence. He is currently undertaking the Masters of Justice (Intelligence) at Queensland University of Technology. His research interests include the use of social media for political activism and terrorism, censorship, policing and law enforcement, and intelligence.

The Challenge of Cyber Crime in India: The Role of Government

Dr. Atul Bamrara

Abstract

Nascent personal computers, high-bandwidth wireless networking technologies and the pervasive use of the internet have transformed the style of performing business. The IT infrastructure provides transmission and storage of gigantic amounts of critical information used in each domain of society and it enables government agencies to speedily interact with each other as well as with industry, citizens, state, local governments and across international boundaries. The paper focuses on an assortment of concerns related to cyber crime and the role of Government to combat the issue. Further findings draw attention to array of cyber crime which is not covered in the IT Act.

Keywords

Cyber Law, Data Diddling, Cyber Squatting, Public Key Infrastructure (PKI), Cyber Stalking

Introduction

The Internet is primarily conscientious for developing and enriching global commerce to previously implausible heights, fostering remarkable advancements in education and healthcare, and facilitating worldwide communication that was once perceived to be limited and costly (McFarlane and Bocij 2003; Jaishankar and Umasankary 2005). However, the Internet, with its immeasurable size and previously unimaginable capabilities, has a gloomy side in that it has opened windows of previously unknown criminal opportunities that not only challenge, but also transcend all physical boundaries, borders, and limitations to sense, rebuke and diminish what appears to be a growing social problem of global proportions.

The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law counterbalanced by the sanction of the state. Computer crime or cyber crime refers to any crime that involves a computer and a network (Moore 2005). The computer may have been used in the commission of a crime, or it may be the target (Kruse and Heiser 2002). Cyber Crime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts (techterms.com). Cyber Crime also includes non-monetary offences, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. The computer may however be a target for unlawful acts in the following

cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in electronic form, e-mail bombing, data diddling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

Symantec defines cyber crime as any crime that is committed using a computer or network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations.

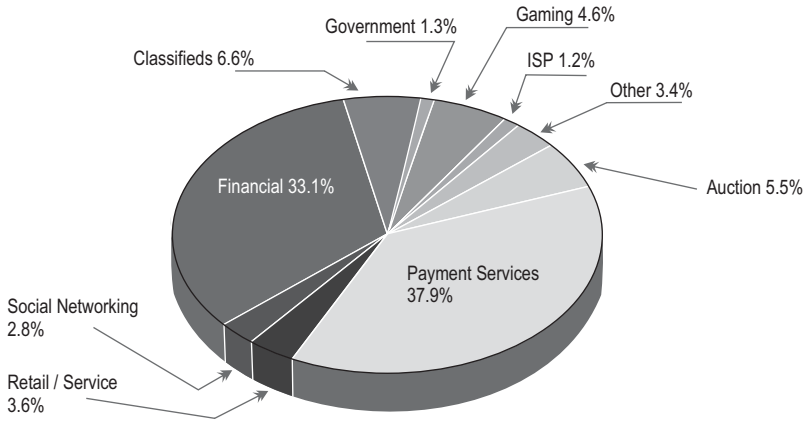
Cyber Crime Challenge

Cyber crime is the hottest and conceivably the most complicated problem in the cyber world. Industry, government and indeed society are becoming vitally dependent on IT (Anderson 1994; Apt and Olderog 1997). This dependence is illustrated by the serious concerns which are now being caused by residual Year 2000 bugs. Seeing that even these conceptually-simple software faults are demanding massive resources, we must be concerned about the much more difficult effects of cyber crimes, malicious activities by hackers or organizations seeking to exploit or disrupt an IT system, for mischief, financial gain, or more sinister motives (Benjamin 1990). Deloitte (2010) revealed a serious lack of awareness and a degree of complacency on the part of IT organizations and perhaps security officers, vis-à-vis the threat of cyber crime. Much of this belief is predicated on the notion that cyber crime technologies and techniques are so effective at eluding detection that the actual extent of the problem may be grossly underestimated. The cyber criminals constitute of various groups/ category.

Today's cyber criminals are increasingly adroit at gaining undetected access and maintaining a persistent, low-profile, long-term presence in IT environments. Meanwhile, many organizations may be leaving themselves vulnerable to cyber crime based on a false sense of security. Cyber criminals are generally computer professionals or computer-literate persons and are not history sheeters and mostly without previous criminal record (Kumar 2002). Studies also show that the threat is mostly from employees or from those with access to the system, such as maintenance personnel, hardware and software vendors, etc. However, external threats via remote access have shown an increasing trend.

The Internet is now available in over two hundred countries and because of its borderless nature. Crimes may be committed through communications that are routed through a number of different countries (U. S. Department of Justice 2000). Although cyber crimes cells have been set up in major cities of the nation but most cases of Spamming, Hacking, Phishing, Vishing remain unreported due to the lack of awareness among internet users and employees of financial institutions.

Figure 1.1 Most Targeted Industry Sectors



Source: APWG Phishing Activity Trends Report 2nd Quarter / 2010

According to APWG Phishing Activity Trends Report 2nd Quarter / 2010, Payment Services was the most targeted industry sector in Q2, as in Q1; enduring nearly 38 percent of detected attacks, up slightly from 37 percent in Q1 2010. Financial Services was second at 33 percent followed by Classifieds at 6.6 percent, though the latter exhibited the most rigorous growth of all sectors in the half. Online Classifieds emerged as a major, non-traditional Phishing sector with almost 7 percent of total Phish. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The internet is very fast becoming a household commodity in India. As more homes have access to internet, more children would be using the internet and more are the chances of falling victim to the aggression of paedophiles. The easy access to the pornographic contents readily and freely available over the internet lowers the inhibitions of the children.

Role of Government

A growing percentage of access is through live connections, users and organizations which are increasingly interconnected across physical and logical networks, organizational boundaries and national borders. As the framework of connectivity has broadened, the volume of electronic information exchanged in cyberspace has grown and expanded beyond traditional traffic to include multimedia data, process control signals and other forms of data. The IT infrastructure has become an integral part of the critical infrastructures of the country. The operational stability and security of critical information infrastructure is vital for economic security of the country. In addition to its underlying role in critical information infrastructures, the IT infrastructure enables large-scale

processes throughout the economy, facilitating complex interactions among systems across global networks. Their interactions propel innovation in industrial design and manufacturing, e-commerce, e-governance, communications and many other economic sectors.

The IT infrastructures' significance to the country has gained visibility in the recent years due to cyber crime and rapid growth in identity theft and financial frauds. These events have made it increasingly clear that the security of the IT infrastructure has become a key strategic interest to the Government. Although the industry is now making investments in security related infrastructure, their actions are directed primarily at short-term efforts driven by market demands to address immediate security problems.

The Government has a different but equally important role to play in cyber security assurance in the form of long-term strategies. In this direction, the deliberations of the National Information Board (NIB), National Security Council (NSC) have stressed the importance of a national strategy on cyber security, development of national capabilities for ensuring ample protection of crucial information infrastructures including rapid response and remediation to security incidents. In the current environment of elevated risk created by the vulnerabilities and threats to the IT infrastructure, cyber security is not just a paperwork drill. Adversaries are capable of launching unsafe attacks on IT systems, networks, and information assets. Such attacks could damage both the IT infrastructure and other critical infrastructures. Cyber security is slowly gaining wider adoption in many consumer products for a variety of reasons. In order to highlight the growing threat to information security in India and focus related actions, Government had set up an Inter Departmental Information Security Task Force (ISTF) with National Security Council as the nodal agency. The Task Force studied and deliberated on the issues such as National information security threat perceptions, legal procedures required to ensure information security, awareness, training & research in information security, PKI infrastructure, information security policy assurance framework and nationwide information security education and awareness program. The primary objectives for securing country's cyber space are-

- Minimize damage and recovery time from cyber attacks
- Preventing cyber attacks against the country's critical infrastructures
- Reduce national vulnerability to cyber attacks
- Actions to secure cyber space include-
- Forensics and attack attribution

- Protection of networks and systems critical to national security
- Early watch and warnings
- Protection against organized attacks capable of inflicting debilitating damage to the economy
- research and technology development that will enable the critical infrastructure organizations to secure their IT assets

The Government is making efforts to identify the core services that need to be protected from electronic attacks and is seeking to work with organizations responsible for these systems so that their services are secured in a way that is proportional to the threat perception. The primary focus of these efforts is to secure the information resources belonging to Government as well as those in the critical sectors. The critical sectors include defence, finance, energy, transportation and telecommunications. Consequently, many in the industry and critical infrastructure organizations have come to recognize that their continued ability to gain consumer confidence will depend on improved software development, systems engineering practices and the adoption of strengthened security models and best practices. Cyber Security Assurance Framework aims to cater to the security assurance needs of Government and critical infrastructure organizations through enabling and endorsing actions.

Rapid identification, information exchange and remediation can often mitigate the damage caused by malicious cyberspace activity. For those activities to take place effectively at a national level, it requires a partnership between government and industry to perform analyses, issue warnings, and coordinate response efforts. The National Cyber Alert System involves public and private institutions to perform analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts. The essential actions under National Cyber Alert System include identification of focal points in the critical infrastructure, establish a public-private architecture for responding to national level cyber incidents, improve national incident response capabilities (CERT-In) and exercise cyber security continuity plans

CERT-In has taken steps to implement National Information Security Assurance Programme (NISAP) to create awareness in government and critical sector organisations and to develop and implement information security policy and information security best practices based on ISO/IEC 27001 for protection of their infrastructure. For communicating with these organisations, CERT-In maintains a comprehensive database of more than 1000 Point of Contacts (PoC) and Chief Information Security Officers (CISO). The technical competency of the empanelled organizations is regularly reviewed by CERT - In with the help of a test network.

CERT-In also conducted a cyber security mock drill to assess the preparedness of organizations in the critical sector to withstand cyber attacks. CERT-In plays the role of mother CERT and is regularly interacting with the cyber security officers of sectoral CERTs in defence, finance and other sectors to advise them in the matters related to cyber security.

Cyber Law and Loopholes

In the Advanced Law Lexicon dictionary, the 'Cyber law' is defined as "the field of law dealing with computers and the Internet including such issues as intellectual property rights, freedom of expression, and free access to information". The Information Technology Act 2000 was introduced on 9th June 2000. The Information Technology Act 2000 came into force on 17th October, 2000. This Act was amended vide Notification dated 27th October 2009. Mitigation that has led to the introduction of the Information Technology Act 2000 was the model law of electronic commerce known as the United Nation Commission of International Trade Law which was introduced in the general assembly of UN by its resolution No. 51 of 162 dated 30th January 1997 which has recommended that all the states should give favourable consideration to the said model law which contained equal legal treatment of user of electronic communication and paper based communication.

Business and knowledge process industries have been growing significantly during last decade in India. However, various incidents of data theft and misuse of private and personal information have raised concerns about outsourcing to India. India does not have a data protection law like US and UK. In the absence of specific legislation, data protection in India is achieved through the enforcement of privacy and property rights. Privacy rights are enforced under the Indian Constitution and the IT Act 2000, whereas the Indian Contract Act 1872, the Copyright Act 1957 and the Indian Penal Code 1860 protect property rights. The Information Technology Act deals with the hacking, tampering with computer source documents, publishing of information, which is obscene in electronic form, child pornography and breach of confidentiality & privacy, while the cyber crime other than those mentioned under the IT Act include cyber stalking, cyber squatting, data diddling, cyber defamation, Trojan attack, forgery, financial crimes, internet time theft, virus/worm attack, E-mail spoofing, Email bombing, salami attack and web jacking.

The IT Act, 2000 penalizes cyber contraventions (section 43-a to h) and cyber offences (sections 65 to 74). The former category includes gaining unauthorized access and downloading or extracting data stored in computer systems or networks. Such actions may result in civil prosecution. The latter category covers serious offences like tampering with computer source code, hacking with intent to cause

changes and breach of confidentiality and privacy. Under the IT Act, a network service provider or an intermediary is liable for any known misuse of third party information or data or for not exercising due diligence to prevent the offence. Therefore, an Indian BPO company may be liable as a network service provider because it acts as a service provider and receives and transmits information or data. The IT Act covers offences and contraventions committed outside India as well, irrespective of the offender's nationality as long as the computer system or network is located in India. Confidentiality obligations are limited to officers or persons having powers under the Act and do not extend to private persons. Further, the officer is not liable to pay off the person damaged by the disclosure. Moreover, most of the penalties are in the range of two lakhs to five lakhs, which are very insignificant amounts when compared to the benefits that an individual may gain by committing crime. The Copyright Act 1957 protects Intellectual Property Rights in literary, dramatic, musical, artistic and cinematographic works. Therefore, copying a computer database or copying and distributing a database amounts to breach of copyright for which civil and criminal remedies can be initiated. However, it is difficult to make a distinction between data protection and database protection under the copyright Act. Data protection is aimed at protecting the information privacy of individuals, while database protection has an entirely different function, namely to protect of the creativity and investment put into the compilation, verification and presentation of databases. India has also witnessed cases of cyber stalking, cyber harassment and cyber defamation but as there is no precise law or provision under the IT Act. A number of cases are either not registered or are registered under the active provisions of IPC which are fruitless and do not cover the said varieties of cyber crime.

Conclusion

Law and enforcement agencies find it necessary to legalize the activities that influence our daily lives with the assistance of science. Laws are persistently being broadened and revised to defy the escalating crime rates. The Government has a diverse but equally vital role to play in cyber security assurance in the form of long-term strategies. Various initiatives have been taken by Government to combat cyber crime. CERT-In, a well quipped organization of Department of Information Technology, Ministry of Communications and Information Technology, Government of India has been established with the purpose of securing countrywide cyber space. CERT-In provides Incident Prevention and Response services as well as security quality management services. The paper focuses on various issues related to cyber crime and the role of Government to combat the issue. In the Information Technology (Amendment) Act 2008, CERT-In has been designated to serve as the National agency to execute the various functions under the umbrella of cyber security.

The author Dr. Atul Bamrara is an academic counsellor in School of Computer and Information Sciences at Indira Gandhi National Open University. His current research interests include Behavioural aspects of cyber crime and wireless telephony, Information & Communications Services in Education and E-Governance issues. His research papers have been published by reputed national and international journals of electronic commerce and information management.

Book Review

Imran Ahmad Sajid

Exposing Sujit Das and His Blasphemous book against the Prophet of Islam (PBUH)

Book Name : Unmasking Muhammad, the Malignant Narcissist and His Grand Delusion Allah

Author: Sujit Das, Mumbai (India),

e-mail : counter.jihad@yahoo.co.uk

Publishing Date: 28.04.2010

Publisher: Australian Islamist Monitor

http://www.australianislamistmonitor.org/uploads/docs/unmaskingmuhammad.pdf

This review critically evaluates the blasphemous book of Sujit Das (Bombay, India), and exposed his venomous character, virulent fallacies, poisonous derivations and out of context narrations and self-styled explanations of many basic and authentic facts about the Holy Prophet of Islam (Peace Be Upon Him). It is a very common propaganda technique of non-Muslims or pseudo free-thinkers of the Muslim world in the modern days to malign Islam, its Holy Book and the Messenger of Allah, Hazrat Muhammad (Peace Be Upon Him), for their petty worldly gains, cheap popularity and ulterior personal motives like cash, publicity, visas, asylum, etc in the western world. The beguiled commentators and perverted writers feel joyous over triggering violent responses from the simple, uneducated and honest Muslim society. Resultantly, these pseudo free-thinkers further capitalize on such uncontrollable demonstrations and a vicious circle of radicalization starts moving round and round. This is how the vested interests further their sinister motives and ensure their mundane gains by creating more and more cleavages in the West and the Muslim world and widening the gap already existing between the two. This review clearly identifies the basic flaws and incoherence in the highly provocative account of Sujit Das, the Dirty (as he names him for Sujit feels no compunctions in uttering very low, mean and base words for the most sacred and holy personality of Islam and all religions, the Prophet Muhammad, Peace Be Upon Him).

It is for the Muslims to try to tackle such writers in an analytical, critical and academic way, and expose their hidden meanness, intellectual dishonesty and superficial understanding of the true and sophisticated Islamic code of beliefs and the essence of its legal system. This superficiality, coupled with malicious ignorance, dishonesty of intention and personal greed, results in such undesirable,

un-warranted and baseless products as that of Sujit Das, the Cursed (only a cursed person can use an abusive language against the holy personalities and prophets). Look at the name of his book: "*Unmasking Muhammad, the Malignant Narcissist and His Grand Delusion Allah*". When the title is so malignant and full of venom and hatred, then what one can expect of its contents to be judged on a scholarly and value-free touchstone.

The Noble Prize Winner poet Rabindranath Tagore who said, in 1924, that "the real cause of the failure of *Brihmo Samaj* was that it lacked a dynamic personality and a practical demonstration behind it". Islam has a very practical personality behind its teachings and tenets in the shape of its Holy Prophet (Peace Be Upon Him). Let us see a few fallacies in the account of Sujid Das' blasphemous account:

1. "Anyone who claims to be a prophet must be prepared to have his Prophesy tested" (p.V).

   Didn't the Prophet of Mercy prove his claim in front of his diehard opponents when he announced his prophet-hood? Why people believed in him then, and why more than 1.3 billion people even today can offer their lives for his respect, dignity and prophet-hood? Were those people mad and lunatics then, and are crazy today? What is Sujit's standards for testing and what is its authenticity, validity and universality?

2. "There are enough pious and totally un-objective traditions of Muhammad preserved by the Muslim religious community, but what is lacking in these sources is honesty" (p.1).

   What about the writings of hundreds of orientalist scholars like AR Nicholson, A R Gibb, TW Arnold, Prof. Phillip K. Hitti, Prof. Montgomery Watt, and many more who wrote very high sounding words in praise of the Holy Prophet and the Holy Book? What is Sujit's criteria for honesty? How can he prove the content and quantity of 'honesty' in his own blasphemous book? Let's see his "honesty". Sujit quotes different rivals of Islam, even of the early Muslim era, the opponents in Mecca and Madina at the time of Prophet's advent, and Sujit firmly believes in all such false accusations with no "testing of honesty" and pretends to have the power of describing all such chronic animosities as a true account! Sujit, and like many others, are not ignorant of the fact that even the worst enemies of the Holy Prophet (PBHM) used to call him *Sadiq* (the truthful) and *Ameen* (the trustworthy), and they used to keep with him their belongings in case of long absence from the village. History is full of such testimony.

3. Sujit casts his sinister aspersions on the first revelation as: "This Divine confrontation was less heavenly and more demonic" (p.3).

   An encounter which happened in a cave for the first time, and unexpectedly, and surely having its awesome spiritual effects, and which later proved to be the starting point of the complete revelation is '*less heavenly*' and '*more demonic*' in Sujit's account. How he differentiates between the spiritual and demonic aspect of an event? With what authority and standard he can say and measure the two portion of being *less* and *more* in one event? A man who has no experience in a heavenly incidence or in a spiritual encounter, how can he realize one from the other?

4. "Muhammad gave no solid proof of his prophet-hood. He simply claimed to the title of Prophet of Allah….How can we be sure that Muhammad didn't lie?" (p.4).

   What is the criterion of a solid proof? When people asked him for proof, didn't Prophet Muhammad (PBUH) present anything? Was he not tested by the excellent and wise brains of his time? Didn't they test him for more than 23 years of his prophet-hood? Were all those believers dump and dupe? Sujit has shown utter ignorance and childish reasoning for proving a case on empirical basis or historical and verifiable proofs. How can we be sure that Sujit is not lying?

5. "Those early companions of Muhammad not only lost their property and self-respect but the lives of their children, relatives, even their own lives. At the end of the day they returned with empty hands, disappointed and disillusioned. All of them were pathetic losers. Almost all of them died a dog's death" (p.208).

   For the rebuttal and denial of Sujit, the Cursed, this one note is enough. Who doesn't know that what was the socio-political conditions of pre-Islamic and pagan Arabia and what made them rulers, scholars, writers, scientists, linguistic experts, administrators, military and political leaders and conquerors? Even the virulent account of the most prejudiced of the orienlatists have admired this humanizing and civilizational force of Islam and its Messenger, the Holy Prophet (PBUH) despite the fact that they don't accept of Islam, and Sujit, the Cursed, has not an idea of any of such marvelous achievements of the Companions and their followers in the initial centuries of Islam. The Muslims must read authentic scholars on Islam and teach their children the true Muslim literature in the current age of anti-Islamic propaganda. The West should not to allow, propagate or protect such sinister and malicious writings and their authors as it damages the efforts of inter-faith dialogue and a joint struggle for solving the problems of humanity and reducing its sufferings.

6. While quoting the great Poet Allama Iqbal that the muslims are in a poor conditions due to their ignorance of the Quran and not properly following the Prophet (PBUH), Sujit says: “If Iqbal is true, then how the infidels have prospered? We, the non-Muslims don't practice Islam at all. In fact some of us even oppose Islam. Then how the infidel countries are better than Muslim countries that at least practice a bit? If the Quran is full of science, then why the Islamic countries are most backward? (p.269)”.

Sujit's account and analogy is full of his superficial knowledge about Islam, Quran, human civilization and the 'Rise and Fall' of dynasties and empires. Iqbal's poetic expression is not untrue when he says that the early Muslims felt and understood the right meaning and message of the Holy Book and became the rulers of the major part of the world of that time. Iqbal has done a copious poetry and he clearly identifies the importance of science and technology for human progress and political dominance. His one part explains the other and shall not be read out of context. Quran is not a book of science but a book of guidance, salvation, enlightenment, moral purification and high ethics and accepted norms for leading a peaceful and productive life. Quran mentions certain guidelines to explore the hidden human faculties and natural resources and exhorts to unearth the forces and energies in the universe, by inviting the human intellect to think about the potential dividends in the globe and universe for further creation and betterment of human life. Quran doesn't provide scientific formulae but a scientific outlook and sets-on triggering a creative vision and analytical thinking in an able-minded person. Sujit's poor knowledge is full of misleading misgivings about Islam and Quran. Unfortunately, the tender, unaware and easily impressionable minds of the young Muslims are unnecessarily polluted and a dis-trust is created amongst the various communities of the world by these atheists and 'employed' writers like Sujit Das and others. Not only the Muslims but also the true academics of other religions should disown and ignore these rubbish and blasphemous writings.[i]

The author Imran Ahmad Sajid is a Gold Medalist in Social Work from University of Peshawar. Currently he is pursuing his Ph.D. Degree from the University of Peshawar. He can be reached at imranahmad131@gmail.com.

[i]For further analytical reading, please read the essay of Mr. Fasihuddin (PSP), the Editor-in-Chief of Pakistan Journal of Criminology which can be accessed through the following link http://www.pakistansocietyofcriminology.com/articles/2012_04_03_325.pdf

Community Engagement

Waziristan Students want Peace and Education

More than a thousand students from North and South Waziristan demanded 'true peace' and 'meaningful education' in tribal areas which could be achieved only if the decision-makers show genuine commitment and sincerity. The students gathered at Raas Gathering Peshawar on the eve of a musical night which was organized by the Waziristan Students Society. President of the Society, Asmatullah Wazir lamented the inadequate facilities of staff, hostels and libraries in the schools and colleges of North and South Waziristan. “Our elected representatives are merely shedding crocodile tears at the agonies of our tribal masses”, said Kashif Dawar, a student leader. Ex. President of the Society Noor Islam Wazir stated that it is absolutely unacceptable to say that the suicide bombers are coming from Waziristan and expressed his anger at the inhuman treatment of law-enforcement agencies especially the police with the tribal people in the cities who are unnecessarily checked and suspected as terrorists. He requested the media not to publish any baseless reports before any findings of investigations as such reports create serious social and psychological problems for the students of Waziristan in settled districts. President of Pakistan Society of Criminology and Patron - in - Chief of Uthman Khel tribe Dr. Fasihuddin was the chief guest on the occasion who urged the tribal students to divert all their energies towards education, acquire modern skills, bridge the gap between tribal population and people of urban areas, persuade their elders to resolve their inter and intra-tribal conflicts, and promote female education in FATA. He advised the students to be the agents of charge in the tribal belt and demanded the government to establish at least one good university in each of the tribal agency and resolve the issue of FATA University as soon as possible.

Full Scale Development for FATA Demanded

Speakers at the large gatherings of Uthman Khel tribe under the auspices of Uthman Khel Qaumi Movement (UQM) at the remotest villages of Mandal and Kharmotay Mosque, Arang in Bajaur Agency stated that poor people of their tribes are being killed and tortured in Karachi but neither compensation is provided to them, nor no national leader has ever come to their native towns in FATA to offer condolence or express sympathies with their bereaved families in FATA. The MQM, being in the Sindh Government, should do proper investigations and shall talk directly to the true representatives of the tribes if their hands are clean, the elders of Uthman Khel tribe demanded at various Jirgas in Bajaur Agency. Central President UQM, Haji Shah Wali criticized the Governor KPK for not doing enough for establishing Bajaur University despite the fact that it is not only the need of the hour but also land has been acquired for the same purpose. Veteran Malak Haji Gul Amin of Mandal said that education, electricity and roads are the immediate requirements of our people as much damage has been done to this area during the war on terror and insurgencies in the last few years. Haji Nasir Khan demanded equitable distribution of development funds and projects in FATA. Husan Bacha deplored the indiscriminate demarcation of boundaries of sub-divisions for Uthman Khel tribe which despite being the largest is reduced to a minority status. Noor Zada lamented the sufferings of the tribal women folk, who in this 21st century are compelled to bring water in pitches from far-flung areas. Shams-ur-Rehman stated that if Uthman Khel sub-sections are united under UQM then no one can stop this warrior but patriot tribe from becoming a force to be reckoned with. Patron-in-Chief of Uthman Khel tribe Dr. Fasihuddin demanded a full-scale development program for FATA and especially the un-attended villages of Momand, Malakand and Bajaur. Being from Mandal section, he was warmly greeted at Mandal. He spoke to different other gatherings of Shamozai and Alizai at Tabai, Barang and Arang also.

Scholars, Poets, Journalists Visit the Historical City of Takht-Bhai

Eminent scholars, famous poets and senior coloumnists of Peshawar visited the historical ruins of Takht-Bhai on Sunday Feb 19, 2012. The visit war arranged by President of Pakistan society of Criminology, Fasihuddin (PSP). The 50 members delegation, including 20 famous lady writers and poetesses of the Women Writers Forum, was led by veteran coloumnist and Secretary General of Abasin Arts Council, Mr. Mushtaq Shabab. Members of the Pashto Literary Society of Takht-Bhai and Uthman Khel Qaumi Movement welcomed the guests. Prof. Pir Zahir Shah and famous Pashto Poets Gul Muhammad Gran, Waseer Lewanay and Javed Khattak presented their poetry and spoke to the guests on the academic and social activities in Takht-Bhai. Later on a Mushaira was held which was the first Hindko-Urdu-Pushto Mushaira in Mardan Division in which poets and poetesses of all the three languages presented their literary work and poetry and received a great applaus. Prof. Nasir Ali Sayed presided over the Mushaira where as renowned author and poet Prof. Nazir Tabbassum performed as stage secretary, well-known scholar, poet and coloumnist Prominent amongst them were Aziz Ejaz (MD, PTV), Ismail Awan, Prof. Hassan Hur, Prof. Sabeeh Ahmad, Prof. Tanvir Ahmad Khan, Sophia Ahmad, Bushra Farrukh, Prof. Ishaque Wardaq, Shakeel Nayab, Hammed Hassan, Rani Bano, Sameena Qadir, Salama Qasir, Zoobi, and many more. It was an excellent gathering of scholar and writers who enriched the audience with their views and melodious poetry.

HIGHER EDUCATION COMMISSION

Sector H-9, Islamabad, Pakistan, Tel: 051-90402428, Fax: 051-90402110
Website : www.hec.gov.pk , Email : slahmad@hec.gov.pk

No.DD/ JOUR/ SS&H /2012/ 216 March 28, 2012

Mr. Fasihuddin (PSP)
Editor, *Pakistan Journal of Criminology*,
Pakistan Society of Criminology
H #3, New Warsak Colony, Ashiqabad, Warsak Road
Peshawar, KPK

Subject: Recognition of *Pakistan Journal of Criminology*, Pakistan Society of Criminology, Peshawar

Dear Editor,

The Higher Education Commission has been endeavoring to raise the quality of research in Pakistan according to international level and research journals are the excellent tool to enhance research capabilities. Research journals serve as forums to present latest research and also for appraisal of existing research. It has been decided to recognize research journals in different categories i.e. 'W', 'X', 'Y', 'Z' as per fulfillment of HEC criteria. I am pleased to inform you that *Pakistan Journal of Criminology*, Pakistan Society of Criminology, Peshawar has been recognized by HEC and placed in 'Y' category (details of different categories are available at www.hec.gov.pk/journals). The HEC is also providing financial assistance to all recognized journals and maximum amount upto Rs.430,000/- per annum would be provided to all 'Y' category journals as per demand. You can apply on the prescribed proforma for funding your journal which is available on HEC website.

The HEC would like to assist you in your endeavors to upgrade the category of your research journal. Since your journal has been graded as 'Y' you will need to address the following issues in order to be considered for up-gradation.

i. Take steps to ensure that each article in your journal is reviewed by at least two reviewers (including one international reviewer i.e. from academically advanced country in the respective discipline and policy of Blind Review should be followed strictly.
ii. In addition to EBSCO, it is proposed that the journal should be Abstracted/Indexed internationally with other HEC Recognized agencies as well.
iii. To prevent plagiarism and ensure original research in your journal kindly use anti plagiarism software 'Turnitin'.
iv. The journal may be included in ISI's Master List.

We would also like you to take steps to place your journal online to allow international access to its contents. Technical help can be extended to you for this purpose if you so wish.

With profound regards,

SULAIMAN AHMAD
Deputy Director (Academics)
Social Sciences & Humanities Research Council of Pakistan

Distribution:
1. The President, Pakistan Society of Criminology, Peshawar
2. Office copy

Pakistan Journal of Criminology

Volume 3 / Number 3 / January, 2012

Contents

Causes of Radicalism and Responses in Pakistan

A Note from Editor-in-Chief

Comments from the Guest Editor

Dr. Geoff Dean (Australia)

Policing the Perilous Euroland: Countering Terrorism and Radicalization in Europe

Monica den Boer & Irene Wiegand

Social Network Analysis of Terrorist Networks: Can it add value?

Mark Lauchs, Robyn Keast and Vy Le

Assessing Terrorist Risks: Developing an Algorithm-Based Model for Law Enforcement

Frederic Lemieux and Regens

Terrorism Investigations in Pakistan: Current Perceptions and Realities of Frontline Police

Fasihuddin

Are Suicide Bombers Coming from Madaris (Islamic Schools) in Pakistan?

Fasihuddin and Imran Ahmad Sajid

The Dark Side of Social Media: Review of Online Terrorism

Geoff Dean, Peter Bell, Jack Newman

The Challenge of Cyber Crime in India: The Role of Government

Atul Bamrara

Book Review

Imran Ahmad Sajid

ISSN 2074-2738

UNI - GRAPHICS

Pakistan Journal of Criminology

Volume 3 / Number 3 / January, 2012