Terrorism's "Virtual" Safe Haven and the Effects on Terror Operations

Michael Judy
Diplomacy Department
Norwich University
Northfield VT 05663-0367
bearcreekranch@gmail.com

Abstract

ñVirtualò safe havens span the full spectrum of terror operations. The strength and resiliency of the ñvirtualò safe haven is embedded in the inherent complexities of which it is comprised. Understanding ñvirtualò safe havens requires careful consideration of the conditions, resources and demographics that influence their establishment and furthered expansion. Accordingly, the ñvirtualò safe haven resides among the institutional ñgrayò areas which are indicative of the complexities associated with weak and failing governance, e.g. radicalism which enables the transformation of the intangible into the tangible tools of global terror. This ñgraynessò permits terror organizations the ability to operate opaquely and efficiently without the requirement of a formal hierarchy or control mechanism. Therefore, the ñvirtualò safe haven enhances terror operations and functionality through the exploitation of global communications infrastructure, internet technology and the informal value transfer system. In essence minimizing culpability and mobilizing the ñvirtualò safe haven while simultaneously flattening and disaggregating terror operations. Thus, the survivability of the ñvirtualò safe haven is rooted in the shared norms, values and reciprocal trust founded among the ñvirtualò community and the subsequent increase in leaderless terror groups ï the ñlone wolfò. Therefore, governments must relentlessly pursue, and operationalize a comprehensive and efficient counter-terror program that encompasses institutional and organizational interoperability. Governments must mobilize the instruments of cooperation, e.g. diplomacy, economics, information, technology, jurisprudence and military action to facilitate a more responsive and fused inter-agency and international counter-terror policy. In sum, this paper addresses the ñvirtualò safe haven and the effect on terror operations.

Key words: International Terrorism, Safe Havens, Counterterrorism

Introduction

Individual groups who use violence to threaten the U.S., its allies or partners habitually find or create ways to operate without impunity or detection. Whether of private financial means such as narcotics and arms trafficking or harmful political aims or by insurgent, terrorist or other violent extremists, these illicit operations are most successful and dangerous when their perpetrators have a place or situation which provides refuge from efforts to combat or counter them. Such places are often referred to as safe havens. The principles of counter insurgency, counter terrorism, counter narcotics, stabilization, peace keeping and other efforts is to reduce the accessibility, effectiveness and location of such safe havens which afford protection of illicit activities. Agencies in defense, diplomacy, development, law enforcement and other areas all possess capabilities to counter the threat, build capacity and legitimacy of U.S. partners in preventing ungoverned, under governed, contested, misgoverned and exploitable areas from becoming safe havens. To do this requires careful consideration of the geographical, civil, political, and resource factors which make safe havens possible.

This paper focuses on the aspects and key components of ñvirtualò safe havens, more specifically how do ñvirtualò safe havens and their key components facilitate terror operations? Additionally, how does the ñvirtualò safe haven add strength and resiliency to terror operations, and what are the counter terror policy implications with respect to ñvirtualò safe havens and their inherent complexities.

Safe Haven

The U.S. government defines a ñsafe havenò as existing among one or more of the following authoritative environments: ungoverned, under governed, misgoverned, contested and exploitable areas of a country. Therefore, understanding safe havens requires some context of simplified definitions: a) Ungoverned safe havens are noted as a weak, failed or a collapsed state, e.g. Lebanonôs, Iranian led and sponsored Hezbollah insurgency; b) Under governed safe havens effectively perform few functions, e.g. Kurdistan-Iraqôs and nationalist movements of the PKK, KDP and PUK; c) Misgoverned safe havens are pervaded by corruption, illicit activities and right-wing terrorism, e.g. Afghanistanôs and Iraqôs Islamic Republic struggle against Taliban and al-Qaeda radical Islam; d) Contested safe havens provide none of the basic functions of governance due to a lack of capacity, or relinquishment of authority permitting illicit actors the ability to perform some governing functions promoting ideology, security and popular support, e.g. The West Bank, Gaza Strip and Beeka Valley under the provisions of Palestinian Authority lying within Israeli territory; e) Exploitable safe havens comprise a functional government and supporting pillars, but permits illicit actors the ability to exploit social, legal and cultural norms to the benefit of the populace, e.g. Tri-Border area of Brazil-Paraguay-Argentina known as the ñIguazu Triangleò (Lamb 2008, 17).

As a result, illicit actors seeking to establish safe havens converge on geographical situations which afford cover. Cover which manifests itself of corruption, disunity, oppressive rule, social and political insecurity and instability, economic and educational disparity, social and political upheaval. A political situation that provides breathing room for spreading radicalism and dissent among the disenfranchised populace, and a population that is willing to ñlook the other wayò. In essence, ceding the future to ulterior radical ideology in lieu of self-governance and rule, additionally, the illicit actor requires resources to establish operating capacity and functionality among the newly found safe haven. This then creates a complex web of interconnected key components which facilitate terrorist safe havens. Accordingly, safe havens trend along the interstices of governmental ñgrayò areas such as those mired in provincial, tribal, local or autonomous institutional insecurity, radical jurisprudence, inept legal system, corrupt regulatory framework, sabotaged intelligence, disparate economies and administration that are typically performed by a legitimate institution (Lamb 2008, 15-16).

In context of the ñvirtualò safe haven, those non-physical areas which constitute a threat to the U.S. national security interests whereby terrorists are able to organize, plan, raise funds, communicate, recruit, train and operate in relative security. This is due to inadequate government capacity, political will or both. In essence, the efficacy of governance may well define a stateôs susceptibility to terror organizational influence and infiltration in establishing ñvirtualò safe havens. ñVirtualò safe havens exist not in the physical sense, but in the literal sense, whereby real humans exploit physical, political, social, economic and religious infrastructure to operate. This is conducted without regards to geographical terrain, but through physically diffuse networks consisting of local and wide area computer networks, mobile phone systems, media communications outlets, informal transaction and banking, and various forms of information dissemination. In doing so, terror organizations exploit a wide variety of developing technologies to meet their organizationôs needs. With emerging and developing technology, terror organizations have unlimited resources at their disposal, .e.g. encryption, password protection, digital imagery, embedded messaging, 3D review and rehearsal, online chat-collaboration, electronic drop boxes, etc. ñVirtualò safe havens emulate the real world and permit the establishment of ñvirtualò communities, economies, political affiliations, religious flocks, social networks, etc. without the constraints of regulation, tribal hierarchy, or traditional cultural norms. Therefore, the logic of ñvirtualò safe havens creates a fog of ñunknown unknownsò which surrounds terrorismôs network of networks. This phenomenon is a bizarre mutation of both intangible and tangible components and resulting complexities which facilitate global terror operations (Global Focus 2010, 1).

Functionality of the “virtual” safe haven

The utility of a ñvirtualò safe haven is foreseen as a non-physical area whereby illicit activity is garnered in support of terror operations through a network of networks amidst a relatively secure environment. The ñvirtualò safe haven is comprised of components such as the internet, mobile phones systems, satellite networks, global communications networks, portable digital media, e-commerce and informal banking which make it possible for individuals and small groups to communicate with each other or with anonymous masses without the requirement for a physical meeting. This makes it possible for transnational illicit actors to undertake global operations opaquely and efficiently. In addition, the ñvirtualò safe haven enables organizations to restructure easily from hierarchal to network while facilitating and developing global operations without the requirement of a formal command and control mechanism. Hence, this permits the spontaneous formation of terror cells worldwide ï leaderless organizations ï that operate autonomously, are inspired by global messaging including the use of virtual training labs such as DVD and websites. Consequently, the ñvirtualò safe haven affords greater flexibility, convenience and security for operations and networking tasks at the individual and small group levels. Tasks include, but are not limited to recruiting, fund raising, communications and information dissemination among other illicit activities (Lamb 2008, 23).

The adaptability of terror organizations to combine the physical world with advances in technology ï the ñvirtualò world - has permitted the spread of semi and autonomous cells throughout the world. Thus, the ñvirtualò safe haven has enhanced terror organization functionality through the use and exploitation of communication, internet technology and funding sources.

Communications

Global communication infrastructure, especially those created by electronic infrastructure such as the internet, media, and unregulated economic activity enables terrorists to fulfill many of the same functions without the need for physical safe haven. These ñvirtualò havens are highly mobile, difficult to track and difficult to control. Therefore, the construct of these decentralized, mobile operations is a testament of terror organizational adaptability and capability amidst the environment of ñvirtualò safe havens (State.Gov 2009, 17).

The impact of mass media communication has greatly affected the overall efforts of global terrorism. For example, the use of audiocassettes delivered Ayatollah Khomeiniôs message to the masses during the Iranian Islamic Revolution while videocassettes brought images of war from Bosnia and Algeria into Muslim living rooms. Training sessions once limited or restricted by time, distance and funding are now possible through the internet. For example, with Microsoft Photosynth the user is able to reconstruct imaging in three dimension (3D) and subsequently ñ3Dò view a scene from varying angles. Merging scenario based internet training, e.g. distant learning, with live training exercises conducted in Afghanistan-Pakistani camps has enabled terror groups the ability to overcome prior constraints and restrictions of informational, logistical and operational needs in executing timely, complex, lethal and non-lethal attacks. Todayôs use of the mass media communication has enabled the more charismatic approach to recruitment and indoctrination through technology, i.e. internet messaging and dissemination reaches an indeterminate number of the masses, circumvents the traditional role of the imam, and advocates various levels of violence to the ñreceptive earsò of the masses. Additionally, the use of chat rooms provides a sense of reality to the corresponding members, creating a ñvirtualò mindset devoid of corruption, exploitation and persecution.

Internet Technology

Internet technology has contributed to the proliferation of websites maintained by terror organizations and the exploits thereof have increased exponentially. As of 1998, only fifty percent of the Foreign Terror Organizations (FTO) listed maintained a website. However, by 2000 all terror organizations had established their presence on the internet (Landman 2010, 12).

For example, al Qaeda launched a web based recruitment drive in 2003 aimed at recruiting fighters to travel to Iraq and attack U.S. and coalition forces. Through the internet a combination of religious decrees, anti-American propaganda, training manuals and instructions on how to make the journey were provided to would-be recruits. The internet serves as the primary tool for intelligence gathering, providing access to a broad range of open source information such as simple maps to aerial imagery. For example, Israeli officials reported that Palestinians were launching rockets into Western Negev from the Gaza Strip using Googleôs popular satellite imagery program ñGoogle Earthò to reconnoiter areas in Israel for targeting. Similar reports came from British forces in the Iraqi city of Basra (Landman 2010, 14).

By exploiting the anonymity and dearth of regulation inherent to the internet, terror organizations have expanded the spread of propaganda, and recruitment of new fighters, but also have taken on more substantive offensives. The use of the internet has enabled the movement of messaging, images and ideals across international borders without interruption in a seamless transformation of terror organization migration. Information is not limited to promotion of organizational logos, ideals and symbology, but also includes the more inflammatory use of weapons, manuals and acts of terrorism, e.g. beheadings, IED attacks, hostages, assaults, etc. (Landman 2010, 15).

The internet remains a repository of topics on how to make explosives as well as chemical and biological weapons. For example, two widely known manuals for explosives are the *'Terrorist Handbook'* and the *'Anarchists Cookbook'*. Additionally, the *'Encyclopedia of Jihad'* provides details on how to establish an underground organization, plan and execute attacks. As technology advances, terrorists accrue a greater capability of learning from real-time information release, e.g. tutorials, etc. essentially establishing a ñvirtualò terrorist training camp (Landman 2010, 13).

As a result, the internet has become the conduit for a terror network of networks, facilitating the global reach and collaborative efforts of a seamless, ñvirtualò operating environment. To elucidate the seemingly benign yet volatile nature of the ñvirtualò safe haven, reference is made to ñIrhabi 007ò - translated as ñTerrorist 007ò. The individualôs real name is Younis Tsouli, and at the time he was a 22-year-old student, but now a guest of Belmarsh Prison in the U.K. Perhaps one might think he was a veteran of the Afghan training camps, or a lieutenant of Bin Laden. Instead, this young individual facilitated communications among terror network groups. Postings by ñIrhabi 007ò included thousands of files online, from videotaped beheadings to detailed manuals for constructing car bombs and suicide vests. Not only had he taught ideology, but the technology of terrorism. As evidenced by the magnitude of investigative resources and efforts allocated to unravel the ensuing plots of ñIrhabi 007ò, it is evident that his individual computer skills were capable of developing a global ñvirtualò network for terrorists and supporters (Landman 2010, 12-13).

More recently, is the release of U.S. classified documents by the internet host WikiLeaks.org demonstrates the vulnerability of national security at the hands of illicit actors and the resulting capability of the ñvirtualò safe haven. This release of classified information reveals the susceptibility of governmental ñgrayò areas regarding information accessibility, systems and the subsequent escalation of compromise to counter terror operations.

Funding

Within the complexity of the ñvirtualò safe haven resides the international underground banking system referred to as the informal value transfer system (IVTS), that which lies outside the traditional banking sector. The IVTS is an attractive system for maintaining anonymity of financiers, which lacks regulatory structure and makes for an underground economy devoid of attribution and culpability. Therefore, terrorist groups are capable of combining technology with internet connectivity to effectively circumvent the traditional banking system recording and reporting of transactions. The reliability, efficiency and availability of IVTS has enabled the transfer of value and goods on a 24/7 basis in a discreet operating manner. For example, the United Nations estimates $200 billion of annual transaction flows through the ITVS, while the World Monetary Fund estimates ñtens of billionsò, and a FinCen report is quoted as saying ñquantifying the amount with certainty is impossibleò (Landman 29-30).

The most well known IVTS is the ñhawalaò system. In recent years terror organizations have used the ñhawalaò system, an extensive informal and untraceable remittance network intended to support illicit or terror operations. Evidence suggests that al Qaeda used ñhawalaò to funnel money into Kashmir valley as well as the bombings of the U.S. embassies in Kenya and Tanzania. The convenience of using ñhawalaò is indicative of its simplicity and ease of use. It is said that users can complete transactions without leaving the comfort of their ñvirtualò safe haven. Thus, the ñvirtualò world of banking and e-commerce are fertile ground ripe with opportunity for terrorist financiers (Landman 2010, 31-32).

Additionally, funding comes from Islamic charities, either because of their sympathy to the cause, or because they believe the money will alleviate the poverty of needy, fellow Muslims. This is further known as Zakat, or the giving of alms according to the third pillar of Islam. In addition, the network raises large sums of money through drug trafficking, smuggling of valuable commodities, extortion, armed robberies and other criminal activities. The ability of terror organizations to sustain operations requires the efforts of funding and financial transactions through the coupling of information technology, communications and associated accounts (Leney-Hall 2000, 10).

The transformation of illicit transactions exploits the weakness of unregulated banking jurisdiction, e.g. limited banking supervision, no anti-money laundering laws, ineffective law enforcement, and ñno lookò policy. These illicit activities are possible via internet listservs and other collaborative platforms online. These platforms essentially make possible intangible economies without oversight, making such illicit activities untraceable (Landman 2010, 31-32).

Component Effects on Terror Operations

Component Effects on Terror Operations encapsulate the synergy of the physical world with that of the ñvirtualò worldôs networks. Networked organizations share three basic tenets: First, that communication and coordination are not typified of vertical and horizontal reporting relationships, but emerge and develop as a matter of the task at hand. Second, internal networks are typically complimented by linkages to individuals outside the organization, spanning national and international boundaries. And third, internal and external ties are not enabled by bureaucratic endorsement, but rather by shared norms and values as well as reciprocal trust ï a ñgrass rootsò level construct. Hence, a bulk of the work is conducted by self-managed teams, while external links comprise a constellation of networks and contributing firms or groups. Several of the most dangerous terror organizations are using technology such as computers, software, hardware, telecommunications, and the internet to better organize and coordinate dispersed activities. Such decentralized activities are indicative of a disaggregated organizational structure, reducing bureaucracy and transitioning to a flatter construct which aligns those groups of a more common goal (Edwards 1999, 35-36).

The implementation of decentralized operations maximizes the concept of ñcost comparative advantageò in planning, coordinating, and supporting terror operations through franchising. IT based mechanisms have facilitated C3I for terror networking and operations through the broader capability of information technology. Advances in IT have increased the speed of communications to real time, reduced the cost of communication and increased the bandwidth of useable spectrum. Through the use of computer conferencing, groupware, internet chat, and web sites participant accessibility is ñhorizontalò and promotes rich exchange without requiring close proximity. The use of IT in a decentralized organization structure enhances the organizational flexibility to change tactics as frequently as possible. Thus, individual groups with common agendas and goals can form subgroups, meet at pre-determined ñvirtualò locations, and coordinate operations, then readily and rapidly disperse. This has further disaggregated the organizational structure to a more autonomous operating cell (Edwards 1999, 30-32).

These emergent ñvirtualò communities afford opportunity, unified in religious precepts and idealized by the mind of users. Without the restraint and face-to-face (F2F) interaction of the social world, the ñvirtualò world allows extreme violence against the presumed conspirators. Collectively, the ñvirtualò community is no longer tied to nationalism, observes no authority other than the Quran and hadith per se, and responds mainly to the mythical umma. The universality of chat rooms reduces the level of discourse to the lowest common denominator, such that within the group each collaborator is empowered as an individual jihadist. Therefore, the use of technology does not constitute a standalone system, but a network of networks which integrates the tangible and intangible components of terrorist operations. These ñvirtualò settings are the precursor to further interaction and development of terror organization movements ï the establishment of network sources and operational cause (Sageman 2004, 155-157).

Effect on strength and resiliency:

I - Terror organizational structuring has flattened as a result of the revolution in communications, internet technology and informal banking during the 1990s has dramatically changed the capability and feasibility of terror networks and operations. During this time, a rapid spread of communication technology occurred providing greater network and operational possibilities to terror organizations. For example, al Qaeda operatives began using laptop computers to store information and send email. Fax transmission was used to deliver communiqués in London from undisclosed locations. Dedicated websites informed mujahedin and their supporters of new developments in the jihad. By the time that the Central Staff returned to Afghanistan in 1996, it was fully integrated into the new global network of networks, which in turn disaggregated and flattened terror organizational structure, making global jihad possible (Sageman 2004, 159).

II - Terror organizational structure has become more decentralized as a result of ñvirtualò safe havens, thus requiring less face-to-face (F2F) interaction. Traditionally, terrorism has been based on F2F interaction, and remains a necessity for long range cellular growth of the organization, whereby the transformation from an outsider to a dedicated insider requires intense intimate exchanges afforded of F2F meetings (Sageman 2004, 157). New technology facilitated global jihad through a decentralized network of mujahedin who transcended the limitations of F2F interaction. For example, the return of al Qaeda to Afghanistan provided a source of outsourced network support through its supply trans management and incorporation of technology into the global jihad, e.g. satellite communication, email, fax, website and computer based information exchange systems (Sageman 2004, 159).

The use of commercial-off-the-shelf (COTS) technology has added multiple layers of protection such as encryption programs, coded email and shared intelligence. Rumors persist that French police have been unable to decrypt the hard disk drive on a portable laptop belonging to captured member of the Spanish Basque organizations (ETA). It has also been suggested that Israeli security forces were unsuccessful in their attempts to crack the codes used by Hamas in sending operational instructions over the internet. Terrorists are capable of sending embedded, clandestine messages within a picture file, encrypted cell phone transmissions, steal cell phone numbers, and use prepaid cell phone cards to secure communications (Edwards 1999, 38).

The overall impact of IT on ñvirtualò safe havens is the lessening reliance on state sponsorship of terrorism and the growing proliferation of autonomous terror organizations whose support is provided through network of networks relying on the ñcost comparative advantageò concept of franchising.

III - Terror networks are 'franchising' requirements along functional lines of ñcost comparative advantageò and the exploits of the informal banking system ï ñhawalaò, e.g. information dissemination, procurement, transportation, recruiting, training, etc. As former Secretary of State Colin Powell once said ñmoney is the oxygen of terrorismò. Without the means to raise and move money universally, terrorist functions are constrained or restricted. Thus, the fight against extremism is primarily focused on the law enforcement, intelligence collaboration and preventing the free flow of money to terror organizations with few constraints. The complexity of terror funding intertwines the concepts of money laundering and operational funding together, i.e. laundering is focused on the source of money, while operational funding is focused on the recipient and application of funds. Therefore, the blending of small innocuous transactions on a daily basis best disguises and reduces detection. Indicators of fraudulent or illicit fund activities are: a) failure to provide accurate and verifiable personal information; b) multiple accounts under the same name, deposits made in multiple accounts that in aggregate are not commensurate with the individualôs expected income; c) multiple same-day transactions using different tellers; d) shared addresses of business locations; e) use of multiple accounts at identical institutions with multiple benefactors; f) use of sequentially numbered money orders; g) accounts which receive periodic deposits and are dormant otherwise; h) and, a dormant account which suddenly goes active depositing and transferring sums of money (Landman 2010, 38).

For example, the 9/11 hijackers exploited the modern financial system using a combination of personal accounts, wire transfers, travelers checks, debit and credit cards. Accounts established and used included foreign financial institutions and U.S. banking institutions such as Bank of America and SunTrust. The sum total transacted in support of the 9/11 attacks was approximately $300,000. Despite the successes of greater regulatory oversight of the formal financial sector, the informal banking system remains open to business for terrorist dollars (Landman 2010, 28).

Summary

A summary of findings points toward a distinct increase in the capability of terror organization networks and operations as a result the ñvirtualò safe haven. The key contributing components of global communications infrastructure, internet technology proliferation and the informal value transfer system inherently improve the redundancy and robustness of terror networks and operations. This occurs as a result of the advances and exploits of science and technology. The rate of technological diffusion, affordability and availability of commercial off the shelf (COTS) items permits the layering of ñvirtualò safe haven capabilities in a shroud of secrecy and unfettered interoperability.

First, the rapid spread of global communication infrastructure and technology has increased network and operational possibilities of the ñvirtualò safe haven. The integration of once incommunicado terror organizations is no longer constrained by the lack of technology dispersion. Global communications infrastructure has created a backbone of commercial and private communication networks capable of bridging the most distant and remote global communication voids. Once fully integrated into the new global communication network, terror operations are adjoined to the global jihad which in turn disaggregates and flattens terror organizational structure, making global jihad possible.

Second, the impact of IT on the ñvirtualò safe haven is the significant reduction in dependency on state sponsored terrorism. The growing proliferation of autonomous terror organizations whose support is provided through networks relies on the ñcost comparative advantageò, or franchising of operational needs. Internet technology has seamlessly breached once impenetrable national, regional and international boundaries of religious, political and militant ideals without interruption or degradation. By exploiting the anonymity and dearth of regulation inherent to the internet, terror organizations have expanded on more substantive offensive terror operations.

Third, despite greater regulatory oversight of the formal financial sector, the informal banking system remains open to business for terrorist dollars. The IVTS remains a lucrative and efficient system for skirting culpability, and acting with impunity in evading regulation which makes for a virulent underground economy. Thus, the combining of communications, technology and internet connectivity terror organizations circumvent the traditional banking system. The IVTS is the method of choice for terror organizations participating in illicit activities and operations as a secure, reliable and convenient means.

Lastly, the ñvirtualò safe haven permits uninhibited restructure, the spontaneous formation of terror cells worldwide and leaderless organizations that operate autonomously with minimal constraint or restriction. The adaptability of terror organizations to combine the physical world with the ñvirtualò world has permitted the spread of global jihad. Thus, the ñvirtualò safe haven has exponentially increased the complexity of terror networks and operations.

Conclusion

To successfully combat the establishment of ñvirtualò safe havens requires both a broad range of domestic and international counter terror strategy and operational procedures. The range of effort must focus more intently on the forensic or micro engagement strategy that accentuates the concept of ñforward trackingò and ñback trackingò of ñvirtualò safe haven component sources and applications; in effect, closing the loop on investigative leads and requirements in the struggle to curtail the proliferation of terror networks and operations. This combined strategy and operational approach will institutionalize the ability of government to grapple with the complexities posed of intangible and tangible resources, people and conditions which proliferates the establishment of the ñvirtualò safe haven.

A successful counter terror strategy requires a three pronged approach: to deny, disrupt and reduce ñvirtualò safe havens. The denial, disruption and reduction of ñvirtualò safe havens will lead to an overall degradation of global terror operations by eliminating or restricting accessibility to communications, internet technology and funding assets which permeate and permit the further exploitation and creation of global ñvirtualò safe havens. This dual-edged sword must balance between the illicit application of key components in relation to the fundamental sustainment of industry, trade and commerce, monetary and fiscal practices, education and information dissemination, etc. with that of regulatory oversight and enforcement. To meet the threat head-on, counter terror strategy and operations must navigate the hypersensitive issues surrounding areas of personal privacy and corporate proprietary information, profile screening and verification, jurisdiction and jurisprudence, international law, investigation and extradition, and sovereignty as it affects the use and collaboration of global communications, internet technology and the informal value transfer system.

The fact remains, a state may contain more than one form of ñvirtualò safe haven based on its demographic, socio-economic, politico, religious and cultural conditions. In addition, these associations may overlap various boundaries internally and externally, adding layers of complexity in identifying the key contributing components to the establishment of the ñvirtualò safe haven. Simply stated, safe havens exist as a combined result of people, resources and conditions. A ñvirtualò safe haven exists because someone desires it to exist while simultaneously the government is incapable or powerless in denying, disrupting or reducing its establishment. In all cases, understanding the people, resources and conditions is central to understanding why ñvirtualò safe havens exist (Lamb 2008, 23).

Therefore, counter terror strategy and operational challenge lay in the coalescing of various agency, department and institutional efforts. The coalescing of domestic partners such as the departments of: state, defense, justice, interior, homeland security, treasury, information management, etc. in close concert with international community partners such as the International Criminal Court, Court of Justice, Interpol, etc. In all, the counter terror strategy and operations must provide resilient and lasting preventive and corrective measures which are suitable for implementation given the necessity for reversing ñvirtualò safe haven conditional pretenses.

Bibliogrpahy

Edwards, Sean. *The Networking of Terror in the Information Age.* Rand Organization, July 1999, Accessed 29 July 2010, Web. http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch2.pdf

Global Focus Organization. *Al Qaeda Dossier.* Accessed 7 July 2010, Web. http://www.globalfocus.org/GF-Al-Qaeda.htm

Lamb, Robert. *Ungoverned Areas and Threats from Safe Havens.* Office of the Under Secretary for Policy Planning, January 2008, Electronic

Landman, Stephen. *Funding Bin Laden's Avatar: A Proposal for the Regulation of Virtual "hawala"s.* Accessed 28 July 2010, Web. http://www.terrorfinance.org/files/virtual-òhawalaòs.pdf

Leney-Hall, Katya. *The Evolution of Franchise Terrorism: Al-Qaeda.* Hellenic Foundation for European and Foreign Policy, 2000, Working Paper No. 1, September 2008, Electronic

Sageman, Marc. *Understanding Terror Networks.* Philadelphia Pennsylvania. University of Pennsylvania Press, 2004 Print

US Department of State. *Chapter 3: Terrorist Safe Havens*. 2009*,* Accessed 29 July 2010, Web. http://www.state.gov/documents/organization/65466.pdf