2009

Identification of Transnational Threats

Stephen R. Bowers
Liberty University, srbowers2@liberty.edu

Stephen M. Parke
Liberty University, smparke@liberty.edu

Identification of Transnational Threats

Stephen R. Bowers
Stephen M. Parke

Executive Summary

In the past, the starting point for threat identification was the nation state. Today, national boundaries have lost much of their significance and global forces lacking identifiable national frontiers represent a real threat to US security.

New technologies have facilitated the development of advanced terrorist methodologies and tactics.

A new and increasingly significant threat is hostile forces which operate within the borders of states which are friendly to the United States.

American universities are increasingly vulnerable to new transnational threats by virtue of the opportunities they present for acquisition of dual use technological skills.

With its new cellular structure, terrorism has been privatized, is more difficult to counter, and enjoys great access to funds, weapons, and training.

The broad anti-war coalition has created threats to the US critical infrastructure in connection with "direct action" against the Iraqi war.

In one year alone, computer criminals funneled over 2.6 billion dollars out of Russia through Cyprus.

Traffic in false documents constitutes an especially significant threat to our critical infrastructure and has become more serious with technological advances that have eased the production of such documents.

The rise of identity theft, an important variation of traffic in false documents, threatens to undermine an important infrastructure base.

Identification of Transnational Threats

Stephen R. Bowers
Stephen M. Parke

Transformation of Threat Analysis: Basic Assumptions

The starting point of this analysis is the assumption that there is an essential linkage between policy research and actions. Therefore, if one accepts that there is such a thing as a transnational threat, it is incumbent upon that person to identify the specific threat. If that threat can be identified the logical next step is to engage in an analysis of the identified threat by utilization such tools as a terrorist typology. Finally, if all these steps can be accomplished, one is left with a duty to respond.

The latter obligation, however, is the most difficult because there is no international or even national consensus to impose sanctions against nation states or even companies that support terrorists or terrorism. The fact that in recent years nations such as Germany and France have provided support to Iran and Syria even as those regimes have been implicated in terrorist activities directed against the West.

The first step in this analytical process is to recognize that the transformation of the international arena has completely altered traditional threat analysis scenarios. In the past, the starting point for threat identification was the nation state and analysts could conduct examinations based on readings of the activities of any state which could have an impact on US security. Today, national boundaries have lost much of their significance and global forces lacking identifiable national frontiers represent a real threat to US security.

At the same time, the intentions of forces which threaten national security have also changed. During the Cold War era, US policy makers saw world domination as the eventual intent of our adversaries. In this new environment, global forces such as Islam aim at nothing less than the destruction of Western societies that they view as fundamentally corrupt and totally beyond hope of reform or redemption. In his book, *Militant Islam Reaches America*, Daniel Pipes writes that "there is…no comparable threat today" to that posed by militant Islam. This situation, Pipes argues, is not simply the result of Western foreign policies

perceived as "anti-Muslim" but is derived an Islamic realization that the glories of previous centuries – with their stunning combat victories and great prosperity - have been lost. "In modern times, those battlefield victories have been lacking, as have prosperity and scientific breakthroughs," Pipes writes. [1] He explains that the modern Islamic trauma has been exacerbated by a realization that, while Muslims constitute 20% of the world's population, they make up over half of the world's 1.2 billion who live in live in abject poverty. [2]

While goals have changed, the tactics employed by our adversaries are no longer based on conventional military strikes that can be deterred via traditional strategies such as containment, massive retaliation, or flexible response. Contemporary global forces are increasingly inclined toward the utilization of transnational terrorism as a weapon to counter Western military and economic might. In such an environment, the deterrent instruments created by Western militaries lose the potency and relevance that enabled them to effectively counter the Soviet military and political threats of the Cold War.

Terror has been privatized and cells can now operate independently. This has resulted in a paradigm shift in how they operate. Their use of internet and other methods of communication has made an enormous tactical difference and forever changed the dynamics of counterterrorism efforts.

[1] Daniel Pipes, *Militant Islam Reaches America*, New York: W. W. Norton, Publishers, 2003, pp. 3-4

[2] Daniel Pipes, "Islam and Islamism", *The National Interest*, Spring 2000, p.87

International Terrorism and Terrorist Typologies

The transnational threat may come in any one of several forms and may be expressed in various ways. Consequently, there is an abundance of categories designed to express the essence of those forms. One typology classifies the terrorist threat in terms of the relationship of the group to a nation state. Therefore, we may speak of groups as being state supported, state directed, or non-state supported. In the past, the latter were often less well-trained and less violent than groups with significant state support or direction. More recently, that assumption lacks validity as non-state terrorist actors driven by religious or millennial motivations have embraced excessively violent tactics while enjoying significant financial support for training and weapons acquisition.

Another typology, drawing heavily from sociology, is ordered around the role of the group rather than that of a nation state. With the evolution of the transnational terrorist environment, threat analysis must now concentrate on small units as well as large units such as a nation-state. In this context, we must characterize groups according to their general orientation and recognize that groups are usually in a process of evolution. Accordingly, a group may be created as simply a dissident movement that opposes the ruling state order. The group may even have the formal structure of a rival political party acting within the legal framework for political activism. Closely related to the study of the group are those theories that examine the nature and role of leadership. This variation of group analysis calls attention to the importance of group leadership and, with great frequency, observes that radical leaders are essential to thoroughly radicalize groups. In fact, the group leadership is typically more strident than the rank and file membership of a group.

The essential point is that circumstances may well prompt that traditional political party to adopt a different role. In such a case, a very conventional political organization may become a more militant movement and adopt a dissident stance that demands fundamental changes in the system. Should this rather militant movement become frustrated in the event that its legal efforts to change the system are not rewarded with significant gains, it is likely that the leadership will consider different tactics. It is at this stage that many groups make the leap from legal activism to illegal operations that often take on violent, even terrorist,

features. Such a development would make it possible to claim that what was once a conventional political party had evolved into a terrorist group.

Thus, we must conclude that the constant evolution of groups in a pluralistic environment means that, as we endeavor to identify transnational threats, our analytical framework should accommodate examinations of both macro and micro actors. Moreover, we must be attentive to those circumstances that prompt group transformations. An effective analytical framework will encompass identify (1) large units such as nation-states, (2) individual groups and movements with radical and violent philosophies, and (3) social or economic circumstances that promote radicalization.

In an examination of transnational threats, the purpose of a typology is to offer generalizations that will produce specific threat guidance. What follows is a list that provides an overview of the types of terrorist groups which now threatening US and Western interests. While this list is not exhaustive, it is clear that some of the most common forms are those listed below. In attempting to use this typology, there is one caveat to keep firmly in mind. These classifications are not absolute. Most threats exhibit characteristics that might place them in more than one category simply because movements and organizations often draw support from more than one constituency.

1. **Religious terrorism.** Since 11 September, most discussions of transnational terrorism understandably begin with religiously motivated violence. In fact, in the decade preceding the devastating attacks on NYC and the Pentagon, religious terrorism had emerged as one of the most significant new security threats to the United States. The collapse of the Soviet Union was a crucial event in the appearance of radical Islamic ideologies in Central Asia and the Caucasus region. The demonstrated failure of Marxism as a governing force in Eastern Europe and as a revolutionary force in the underdeveloped world led to a search for non-secular revolutionary ideologies. The failure of Marxism was accompanied by an equally devastating leadership failure in the USSR. Well before the collapse of the Soviet state in 1991, there was a


Hezbollah Activists

generally held popular perception that Soviet leadership had become personally corrupt. In both the Soviet Union and elsewhere, radical Islam gained adherents with its denunciations of corruption and its calls for a revival of true Islamic values. Even more dramatic was the impact of the Soviet invasion of Afghanistan in 1979 and the resultant global calls for Muslims to take up arms. Steve Emerson, a leading authority on the subject of radical Islam, developed the idea of cultural jihad in order to explain the significance of this event.

> The 1979 Soviet invasion of Afghanistan resulted in the first modern incarnation of Jihad on a local level in the Arabic Muslim worlds. No longer confined to a theoretical or simply religious concept, jihad became accessible to young Muslims. One could actually join the jihad and personally participate in a concept that had been elusive, theological and abstract. It now meant that Jihad was attainable at the local level. "Join the Jihad Caravan" was the promotional brochure that flooded Islamic centers and Muslim student groups throughout the United States, promising young Muslims the opportunity of a lifetime. Jihad became the rage. Tens of thousands of young Muslims, from the United States, Europe, the Persian Gulf, the Middle East, and Asia volunteered to fight alongside Afghani mujahideen. [3]

At the same time, the failure of pan-Arab nationalist sentiment also fueled support for radical Islam. In the aftermath of the Soviet Union's military campaign in Afghanistan, the so-called "Afghan Arabs" who had answered the call to join the "Jihad Caravan" emerged as an increasingly influential force in establishing religious terrorism as a threatening and disruptive international phenomenon that operated through trans-national radical Islamic groups.

Religious themes and appeals, it is important to note, are utilized by a variety of violent groups that are not primarily religious groups. For example, animal rights activists such as Gary Yourofsky have often compared themselves to spiritual figures such as Jesus Christ and Ghandi in an effort to gain support. [4] The mere statement of a religious or spiritual purpose does not transform the group into a religious one.

2. **State sponsored terrorism.** Several years ago, Claire Sterling published a book that examined the advent of state terrorism and advanced the thesis that the Soviet Union was responsible for

[3] Steve Emerson, "Jihadism: Where Is It At in 2006", *The Sydney Papers*, 15 February 2006
[4] "Animal Rights Activist Shares Views With Campus". *Indiana Statesman*, April 10, 2003.

most anti-American terrorist activities. This research came amid numerous reports about Soviet and East European terrorist training camps as well as Cuban and Libyan involvement in similar activities.[5] While the Sterling thesis has lost credibility following the collapse of the USSR and the endurance of anti-Western terrorism, it is true that many governments use terrorism as an instrument of foreign policy. They often sponsor terrorist movements. During the Cold War, the USSR regularly supported dissident "national liberation" movements that used terrorism. In the Vietnam War, the US conducted the successful Phoenix program in order to decimate the Communist infrastructure.

The issue of state sponsorship has prompted the United States Department of State to prepare an annual document entitled *Patterns of Global Terrorism* that lists those nations viewed as terrorist either by virtue of their support to terrorist groups or their involvement in terrorist activities. Some typical patterns of involvement are the provision of safe havens for terrorists, operation of training camps, or utilization of terrorist groups as an element of a nation's foreign policy. The annual report also provides a valuable list and description of organizations that have been designated as terrorist.

3. **Left-wing terrorism.** Left-wing groups generally profess a revolutionary socialist doctrine and view themselves as protectors of the people against the "dehumanizing effects" of capitalism and imperialism. Many armed left-wing movements have resorted to international terrorism and have attacked Western institutions and individuals they saw as part of the "imperialist system". They aim to bring about change in the United States through revolution rather than through the established political process. Latin American leftists began the practice of kidnapping Americans during the 1960's and 1970's. They were able to provide funding for their organizations through these often very profitable activities. From the 1960s to the 1980s, leftist-oriented extremist groups posed the most serious domestic terrorist threat to the United States. In the 1980s, however, the fortunes of the leftist movement changed dramatically as law enforcement dismantled the infrastructure of many of these groups and the fall of communism in Eastern Europe deprived the movement of its ideological foundation and patronage.

[5] Claire Sterling, *The Terror Network*, (New York: Random House, 1984), pp. 229-254

Left-wing groups have long been associated with a variety of national and pseudo-national appeals. One of the most common during the post-World War Two period was the movement in U.S. protectorates for "national self-determination." The Puerto Rican independence movement, one of the most persistent left-wing causes, enjoyed consideration attention if not support during this period and employed violence in the pursuit of its goals. The organizations associated with this cause saw terrorism as a legitimate tactic that would bring attention and, eventually, popular support. Among their most dramatic exploits were an attack on the US Congress and a plot to assassinate President Harry Truman. In the 1970s and 1980s, organizations associated with this cause claimed responsibility for a series of bombing incidents in the United States. Those communities that had large populations of Puerto Ricans experienced the most activism by exploiting the concerns and fears of those residents. Eventually, the leaders of Puerto Rican extremist groups lost their enthusiasm and most Puerto Ricans themselves found life in the United State far preferable to any dream of an independent Puerto Rico sought by radical leaders.

Anarchists and extremist socialist groups -- many of which, such as the Workers' World Party, Reclaim the Streets, and Carnival Against Capitalism -- have an international presence and, at times, also represent a potential threat in the United States. For example, anarchists, operating individually and in groups, caused much of the damage during the 1999 World Trade Organization ministerial meeting in Seattle. Their willingness to use violence has made anarchist groups one of the most disruptive forces both in the United States and abroad. Contemporary anarchist movements are building on a rather lengthy tradition in which anarchists have been associated with numerous attacks on U.S. officials and facilities.

4. **Right-wing terrorism.** Right-wing terrorism is less common than many other types of terrorism. While there has been no consistent cycle of rightist terrorism on an international scale it has been more significant on a national basis. This local focus is a result of the fact that such movements are generally rooted in the political and cultural environments of their home countries. One of the better known right-wing extremist groups, the British National Front, makes this clear in its declaration of principals. According to that statement, "We in the National Front strive only to put the interests of British people first, and to create a better

future for our children." [6] They have demonstrated little desire to conduct terrorist activities in order to express solidarity with other right-wing groups.

Right-wing terrorist groups often adhere to the principles of racial supremacy and embrace antigovernment, antiregulatory beliefs. Generally, extremist right-wing groups engage in activity that is protected by constitutional guarantees of free speech and assembly. Law enforcement becomes involved when the volatile talk of these groups transgresses into unlawful action.

There is a variety of right-wing groups, such as Christian Identity Movement, Combat-18, and various militia groups, but they generally do not constitute what would be regarded as a serious terrorist threat. Although efforts have been made by some extremist groups to reduce openly racist rhetoric in order to appeal to a broader segment of the population and to focus increased attention on anti-government sentiment, racism-based hatred remains an integral component of these groups, core orientations. The British National Front, in a one of the Front's anthems, reminds audiences of its fundamental belief when it proclaims "The millennium is new and what do we see? Our beloved old country, the land of the free, Peopled by races from nations diverse, From continents all, every nation on earth." [7]

In the United States, the best-known instance of right-wing terror was the Oklahoma City attack in 1995. There have been other reports of planned or attempted right-wing actions that would have had devastating consequences if actually committed. In 1999, an anti-government group based in California and initiated a plan to attack a large propane storage facility. Had they been able to complete this action, the loss of life would likely have been devastating, well in excess of the fatalities associated with the terrorist attacks of September 11th. At the time of their arrest, group members already had much of the material that would have been required for this action. Later in 1999, the FBI exposed a plan to steal military weapons from a National Guard unit. The plot had been jointly undertaken by several militia groups in Florida, Georgia, South Carolina, and Alabama who wanted to create chaos by attacking power lines in several states and killing federal law enforcement officers who responded to the incidents. The group believed that the federal government would eventually

[6] WWW.Natfront.com/policies.
[7] Ibid.

respond by imposing martial law, an action which would, group members believed, result in a popular revolution against the entire U.S. government.

5. **Special interest terrorism.** Special interest terrorism differs from traditional right-wing and left-wing terrorism in that extremist special interest groups seek to resolve specific, rather narrowly defined issues, rather than effect more widespread political change. Special interest extremists continue to conduct acts of politically motivated violence to force segments of society, including, the general public, to change attitudes about issues considered important to their causes. These groups occupy the extreme fringes of animal rights, pro-life, environmental, anti-nuclear, and other political and social movements. Some special interest extremists -- most notably within the animal rights and environmental movements -- have turned increasingly toward vandalism and terrorist activity in attempts to further their causes. A modern innovation in vandalism has appeared as such movements have created virtual organizations on the Internet and have also employed computer hacking to intrude into the computer systems of companies that have been selected for attacks. As the animal rights activists have enjoyed success in traditional or conventional forms of terrorism in order to disable machinery or sabotage commercial activities, they have used the computer as a way of publicizing their successful attacks.

   Throughout North America and the United Kingdom, animal rights groups have been associated with extreme acts of violence. The Animal Liberation Front (ALF) – an exceptionally extremist animal rights movement – is recognized as one of the most active violent groups in the United States. In spite of the violent nature of ALF's activities, it operates on the basis of a philosophy that discourages acts that harm "any animal, human and nonhuman." In this respect, the organization is similar to many other animal rights groups whose apparent philosophy is contradicted by its violent actions. A distinct but related group, the Earth Liberation Front (ELF), claimed responsibility for the costly fires designed to defeat the plans of resort developers who were, in its view, despoiling the environment. In many cases, such movements have undertaken these actions because the new facilities would deprive certain animals of the use of those forests as part of their natural habitats.

Attacks by animal rights groups have often resulted in the loss of life. Generally, such losses have been associated with efforts to destroy research facilities that might utilize animals for experiments in the development of products ranging all the way from medicines to cosmetics. In the view of many activists, such deaths are justified. One well-known advocate of animal rights, Gary Yourofosky, founder of the group known as Animals Deserve Absolute Protection Today and Tomorrow, recently observed that if an "animal abuser" were killed in connection with any fire-bombings associated with his group, he would "have no problem with that." [8]

Special interest terrorists often select domestic targets that have symbolic links which may be internationally significant. In the 1970s, a Cuban-American group known as *Omega 7* was responsible for over 50 bombings and assassination attempts in the US. Their targets were Cuban diplomats and businesses involved with Cuba. In one well-publicized case in the 1970's, a Cuban diplomat was killed when his car exploded on a street in down-town Washington, DC.

Hostile Groups within Non-Hostile States

While it is fairly easy to formulate a response to the existence of an identifiable threat, the new terrorist environment is one which presents policy makers with dilemmas that defy obvious solutions. Few situations are more perplexing than that posed by the presence of hostile groups or forces operating within what we regard as friendly frontiers. Since September 11th, much has been said about harboring terrorist groups. Given the nature of terrorist organizational strategies today, it is inevitable that there are numerous terrorist groups which enjoy "basing rights" in nations that are not regarded as sponsors of terrorism. In some cases, the presence of a terrorist group will be a matter of explicit and deliberate state policy, as noted above, and characteristic of a nation like Syria. In other cases, groups may operate inside fundamentally democratic nations without explicit state endorsement. The group's presence is simply a result of its exploitation of the laws of an open society.

Britain and France illustrate the phenomenon of terrorists' exploitation of democratic freedoms. Abu Hamza Al Masari, a Muslim cleric who acted as terrorist financier and recruiter, ran a

[8] "ETSU Event Cancelled Due to Confrontation", *Johnson City* [Tennessee] *Press*, April 5, 2002

network based in England. For several years, British authorities ignored his activities because they were not inconsistent with British law. Initially, his network was not seen as a threat to UK security. They finally took action against Abu Hamza, but only after the United States had urged them to do so. Eventually, British authorities used the UK's Nationality, Immigration, and Asylum Act to strip the radical Muslim cleric of his citizenship. Abu Hamza had used his Finsbury Park mosque to call for violence against both US and British interests. [9] Similar terrorist activities are based in France but French authorities are fearful of moving against them because 7% of their population is Muslim. One of the most important French based groups is the Muslim Brotherhood, a radical Islamic group which is banned in Egypt. Founded in Egypt in 1928, the Brotherhood has evolved into an international organization noted not only for its efforts to create Islamic states but also for assassinating political leaders and engaging in clandestine military activities.[10]

The traditional dynamics of international relations work make it difficult to take actions against such groups. As part of the interplay of international politics, our own allies use situations such as this in order to gain leverage with the United States. The seemingly nonchalant behavior in dealing with local Islamic radicals is a means of gaining concessions from the United States. Most nations will move against such a group only in return for specific benefits. As they see it, the Islamic radical group is like a virus which presents no problems for the host nation. Taking action against the virus, arresting its leaders or closing its facilities, at urging of allies may well activate the virus against the host.

[9] "Muslim Cleric Citizenship Revoked", TimesonLine.co.uk, March 5, 2003
[10] Daniel Benjamin and Steven Simon, *The Age of Sacred Terror*, (New York: Random House, 2002), pp. 57-59

Another, more subtle manifestation of this phenomenon is posed by academic programs involving the studies of dual use disciplines or technologies. There has long been a concern about access to technology and information that might be of value to terrorists. [11] It is obvious that a great deal of sensitive information can be acquired in academia. This approach represents a respected and thoroughly legal way of obtaining data that otherwise could only be acquired via the methods of espionage. One recent and very telling illustration of this involved the case of Sami al-Hussayen, a student at the University of Idaho, who was acquiring a PhD in Computer Science with a specialization in computer security and intrusion techniques. Al-Hussayen was an active member of the Islamic Assembly of North America (IANA), managed six bank accounts in the US which transferred large amounts of money to and from radical Islamic groups, and registered and maintained radical Islamic web sites for the IANA. Before September 11th, one of his web sites talked about "bringing down an airplane on an important location that will cause the enemy great losses." [12] The IANA is only one of many such groups which operate on US campuses. Others, such as the World Assembly of Muslim Youth and the World Muslim League, have already gained attention because they are funded and tightly controlled by the Saudi government and the Wahhabi clergy. Together, these and other similar organizations present a picture of a university environment which, by virtue of the freedom required for its effective operation, is increasingly vulnerable to a new type of threat. [13]


Sami al-Hussaven

For over a decade there have been numerous warnings about Islamic terrorist groups operating within the United States. These groups use American freedoms in order to undermine that free system. In the current international environment, a potential terrorist no longer has to find a foreign territory from which to launch an attack against a nation such as the United States or the United Kingdom. The 9/11 attackers came into the United States through the front door. The May 2007 terrorist plot against Fort Dix was planned by US based terrorists who had no

[11] Zachary S. Davis, "Weapons of Mass Destruction: New Terrorist Threat", Congressional Research Service, 97-75 ENR, January 8, 1997
[12] "What Price Diversity?", www.UIDAHO.edu, March 13, 2003.
[13] It is worth noting that Huda Salih Mahdi Ammash, the developer of Iraq's biological weapons program, was trained at US universities.

connections with Al Qaeda. According to the FBI, dozens of homegrown terror plots have been uncovered by local law enforcement.[14] The perpetrators of the 2007 attacks in London and at the Glasgow airport were legal UK residents. As long as a person can get a passport and a visa, he has no need to sneak in across the border illegally hoping to contact local sympathizers.

Operational Methodologies and Tactics

1. Criminal activities. Crime constitutes and operational methodology because terrorists are involved in criminal acts as a way of financing their objectives. It is important to note that all terrorism is criminal although all criminals are not necessarily terrorists. If a group's primary motivation is profit, it is reasonable to characterize that group as criminal in contrast to political. Groups that should be characterized as criminal terrorists have often been involved in terrorist activities in the course of their criminal endeavors. Most scholars have been inclined to view these activities as exceptional for criminal groups because most of them want to avoid publicity. It is the nature of criminal terrorists to be anonymous and to involve themselves in terrorism primarily as "sub-contractors". The key identifying element for criminal terrorism is motivation.

Criminal organizations are most often involved in terrorism in one of two important ways. First, they are essential to the production of the false documentation upon which terrorists rely in order to travel freely and maintain their covers when operating in target countries.

A second type of criminal activity that is frequently associated with terrorism is kidnapping. While less essential than the production and maintenance of false documents, kidnapping has long been used as a way of financing criminal actions, including terrorism. Much of Latin America and Asia has experienced severe "epidemics" of kidnapping. In both regions, paramilitary groups and other terrorist organizations have taken the lead in conducting kidnapping operations.

The Central Asian experience is especially instructive in demonstrating the complex factors driving this phenomenon. First, kidnapping in Central Asia is long been motivated by three factors: tradition, profit, and politics. The role of tradition is

[14] "Homegrown Terror a Threat in United States", *US World News*, 14 May 2007

illustrated by what is known as bride kidnapping. This was a traditional practice throughout Central Asia, but especially in Kyrgyzstan, in the pre-communist era. Bride kidnapping was a cultural phenomenon and it had no political significance. In the post-Soviet era, bride kidnapping has reappeared without any of the romantic notions of that earlier period and is generally little more than a euphemism for rape.

Within a period of just a few years, kidnappings assumed both political as well as purely criminal dimensions. The phenomenon assumed a political coloration when rival groups began to practice kidnappings and hostage takings against each other simply as a way of conducting their political contests. By the time of the civil war in Tajikistan, kidnapping and hostage taking widespread problems that posed a major challenge to the region's post-communist development. The terrorist groups engaged in such actions were not punished and hostage taking assumed massive proportions. While outsiders, especially Westerners, were the most sought after targets, Central Asians themselves were the most frequent victims. Influential political and religious leaders and their families, businessmen and members law-enforcement bodies are among the most likely targets of abductions. Hostage taking has been an especially useful tool for putting pressure on political opponents. Political demands generally accompany political hostage taking. The number of kidnappings of high-level hostages with political aims has been increasing for over a decade in Central Asia.

The aim of political abductions, involving both opposition and pro-governmental forces, was either removal of important persons of the opposition party or obtaining secret information about the plans, activities and resources of the enemy. However, when the civil war ended in the mid-1990s, the main aim of abductions was financial gain with little consideration of political goals. There were also frequent demands to free other criminals who were being held in prison.

2. United Fronts or Radical Coalitions The creation of united fronts and collations is another common operational methodology. As noted above, movements often set out to generate support for their cause by finding more than one constituency. When the United States became involved in military operations against Iraq, anti-war groups in the U.S. attempted to disrupt essential services. In doing this, the anti-movement embraced a variety or organizations. It is somewhat difficult to

categorize the anti-war movement because it constitutes a coalition of radical groups. Many alliances are composed of seemingly incompatible groups that have made common cause for specific or limited objectives.

The disparate anti-war movement finds individuals from the extreme left suddenly united with followers of the extreme right. Anti-globalists students join anti-foreign, isolationist supporters of Pat Buchanan. Black radicals whose formal education stopped in middle school march along side university professors whose regular haunts are the halls of academia rather than impoverished inner city neighborhoods. Their ranks are further increased by radical lesbian groups who join with a variety of gay rights organizations, none of which would ordinarily seem to have a foreign policy agenda. This broad front also includes Radical Greens who argue simply that war is bad for the environment and the Marxists who see war as evidence of the failures of capitalism. Because the war took place in the Middle East, the front has also been embraced by anti-Semites who hope this is another chance to push U.S. foreign policy against Israel. Animal rights organizations have become part of the anti-war coalition if only because it provides another opportunity to popularize their cause. The US Navy's utilization of dolphins in de-mining operations as the US forces moved into Iraq gave the animal rights organizations a useful platform for this effort. Finally, there are foreign governments who seize on this as an opportunity fuel dissension within the United States as well as terrorists who want to view U.S. police forces in operation from this close vantage point.

Anti-war march, 2003

The anti-war movement has demonstrated an ability to focus on weaknesses in the U.S. critical infrastructure. During the Iraq war many of the activists in this movement declared their intention to "shut down the war merchants" as a form of anti-war protests. One example of this effort was illustrated by a group called "Direct Action to Stop the War" which set out to block supplies to US military forces from being shipped out of the Oakland port facility. The target of this action was a cargo carrier that had contracts to ship military supplies. The group called on members of the International Longshoremen and Warehouse Union to honor a picket line set up by demonstrators.

While the union had been noted for its anti-war stance during the Vietnam conflict, its members chose to honor the contract with the US government. When peaceful efforts failed, many of the anti-war groups turned to violence and San Francisco experienced several days of clashes that disrupted many of the city's basic services. In a downtown alley police found a dozen Molotov cocktails ready for use if they had not been discovered. The financial center was deadlocked when traffic on the Bay Bridge was snarled and threats by cyber terrorists caused great concern among the banking community. [15]

Environmental activists joined in the anti-war violence with attacks on sport utility vehicles (SUV). According to Earth Liberation Front, the SUV was a significant factor in the Iraqi war because it generates a greater need for gasoline and this need, in turn, helped justify what anti-war spokesmen described as a "war for oil." In particular, the ELF has been associated with the vandalism of SUVs, both those on the lots of automobile dealers as well as those already being driver by consumers. In one incident in Santa Cruz, California, sixty-five SUVs were vandalized while other attacks took place in Pennsylvania and Virginia. ELF representatives, while not claiming credit for these actions, did observe that they were "consistent with actions that the ELF has taken in the past in opposing the war and opposing SUV over-consumption." [16]

The umbrella group that was created to facilitate this wave of demonstrations is known as International A.N.S.W.E.R. It was created with the financial and organizational backing of the Workers' World Party. The WWP leadership is well known for its support of North Korea, a state which, in the words of WWP official Deidre Griswold, enjoys popular support because its leadership "has kept it from falling under the sway of the transnational banks and corporations that dictate to most of the world." When Slobodan Milosevic's trial began at the International Criminal Tribunal in The Hague, Netherlands, the organization pledged its solidarity with the defendant and denounced the 'trial' as a NATO frame up." The WWP is a very small group whose leading members have traveled regularly between Pyongyang, Havana, and Baghdad, raising funds for anti-war activities while stressing that such regimes should be praised because of their resistance to the forces of "globalism." [17]

[15] MSNBC News broadcast, 7 April 2003
[16] "Anti-war Vandals Hit SUVs", *San Francisco Chronicle*, April 11, 2003, p. 1
[17] "Who Pays for These Demonstrations?", Stephen Schwartze, FrontPageMagazine.com, January 24, 2003

3. Cyber terrorism and information warfare These operational methodologies generally do not generally involve physical violence but their potency for disruption is a function of the sophisticated nature of modern society. In a relatively primitive system, we would not be alarmed by an adversary's utilization of such tactics.

When a federal jury in the Northern District of Texas convicted Bayan Elashi and his colleagues on charges of conspiracy to support a terrorist organization, they employed a technology that would have been unimaginable a few years ago. While terrorists in the past resorted to blatant acts such as bank robbery, Bayan Elashi helped created Infocom, an internet service provider which was working as a front for Hamas and helping channel money to the radical violent group. [18] The case was neither new nor distinctive but simply an illustration of a marriage of technology and terrorism.

By the early 1980s, modern societies were enjoying the benefits of new technologies that revolutionized the way in which information was collected, processed, stored, and searched. These technologies redefined the way our modern, global society operates. At the same time, the new technologies also created new opportunities for terrorist groups to operate in regions and employ methodologies previously beyond their reach.

When the Westernized nations were first caught up in this dramatic development, much of the world was excluded from this dramatic innovation. For example, entry was barred to the communist party states of Eastern Europe. Prior to Gorbachev's policies of glasnost and perestroika, Soviet citizens were not allowed to own even the most rudimentary computer. In fact, the only computers used in the USSR were huge ones provided for offices. That ban was lifted, in part, because young Soviet citizens demonstrated an ability to make their own computers and, moreover, because Gorbachev's reformers did not want Soviet citizens to be left behind in the computer revolution. During the remainder of the Soviet period, there was still the restriction posed by KGB monitoring of most activities conducted on personal computers. Computer users were also limited by the fact that, in those early days of the information age, only Soviet computers were available.

[18] Department of Justice, Press Release 1 December 2005, www.USDOJ.GOV, p. 2

Both Eastern Europe and many nations of the "third world" entered the "information sphere" as limits on private information technology were finally lifted and there was a corresponding dramatic drop in the price of personal computers. Today, the communications and programming industries are among the most dynamic sectors in the post-communist economies as well as in many regions of the Middle East and Asia. A city such as Moscow, for example, can now boast of having over one million personal computers and other cities throughout the "third world" are not far behind the Muscovites.

However, the popularity of personal computers has created a new problem: computer crime. According to law enforcement authorities, skilled hackers (who are often paid by the robust criminal organizations) have the skills needed to easily break almost any code, thus gaining access to valuable commercial secrets. Using these methods, one Russian citizen, acting independently from his home in St. Petersburg, used a personal computer to steal over 10 million dollars from the New York-based City Bank of America. Criminal elements in Nigeria employed these methods in order to target the bank accounts of thousands of citizens in North America and Western Europe. The breadth of this problem was revealed in a report produced by the United States Institute of Computer Safety that stated that 85% of all large American companies had reported violations of their computer security systems. It was this situation, of course, that prompted US President George Bush to set aside four billion dollars in an effort to safeguard the information systems of the USA.

Experienced Internet users are generally aware of price lists indicating how much it would cost to break into a particular network. For example, a person can pay $800 to a skilled hacker in order to obtain a database from a typical Linux configuration. People involved in such activities are not likely to be paid by local criminal organizations but rather by international groups. Most criminal organizations have only local interests. In the former USSR and the "third world", there are fewer significant local E-business or other important systems such as the FBI or NASDAQ to penetrate. Therefore, the targets are more likely to be international and, consequently, the sponsoring organization is likely to be an international one.[19]

[19] Interview with Dr. Vasile Nedelciuc, director of software firm in the former USSR, Chisinau, Moldova, April 21, 2003

In one year alone, over 2.6 billion dollars, from a variety of international sources, was funneled through Russia to Cyprus. The location of Cyprus is significant and underscores the complicated interactions between different types of terrorist and criminal activities. By the late 1980s, Cyprus had become a major transit point for weapons that were funneled out of the Bekha Valley into other terrorist hotspots. The illegal Russian funds are clearly of great significance in facilitating the transfer of terrorist weapons into a global market. [20]

Because the arrival of computer technology in the former Communist Party states was delayed, the information security situation in Eastern Europe differs from that in the West. A consequence of this delay is that the region's reliance on information technologies is less advanced in the East and, therefore, computer crimes represent less of a problem. This, of course, is certainly true in terms of the amount of money lost as a result of such activities.

By the time Eastern European nations were developing modern banking systems, there was a clear realization of the extent to which computer security was vital as well as an understanding of banking vulnerabilities. Consequently, East European banking systems are being developed with a greater emphasis on information confidentiality. Planners have learned from the Western experiences with information crime and have done more to limit outside access to their systems. Thus, it seems that the threat of information crime – while present – is less acute in the East than in the West. Faced with smaller and more secure targets in Eastern Europe, most of the region's computer criminals have chosen to prey on Western information systems.

Computer crime generally falls into four categories:

1. **Theft of computers and their components.** Usually taken from the places where the computers are either made or assembled, these stolen computers and their components are sold on a black market. Since computers in general and microprocessors in particular, are expensive, their theft has created a very lucrative business for criminal elements. In addition – microprocessors do not have serial numbers, which makes their retrieval by law enforcement personnel very difficult. The cost of the theft of computers and their components has been

[20] Interview with retired FBI official, C. Glen McWright, Washington, DC, April 16, 2003

estimated as no less than one hundred million dollars per year in terms of their value in a market such as that in Eastern European.

2. **Computer piracy.** The illegal copying of computer programs to be sold on the black market or for personal use is a major business in Eastern Europe, Asia, and the Middle East. In fact, it is likely that over 90% of some very expensive programs in these regions are being used without licenses.

3. **Illegitimate access.** The use of different computer systems in order to damage or destroy information in other systems is a common practice in the region. This is accomplished when a computer hacker accesses a computer system and uses it for his own purposes. While hackers are often motivated by profit, not all hackers have such intents. Many see breaking into a system as a challenge, and once they have done this, they leave the system unharmed and seemingly untouched. Others hack into systems in order to test the safety of the system. Many use their computer skills in order to make free phone calls all over the world.

4. **Use of computers in order to commit illegal acts.** Among the most common acts undertaken by hackers are the fraudulent uses of e-mail advertisements, false claims, or the securing of false identities. An increasing number of individuals hack into systems in order to commit acts of sabotage. The paradox of computer crime is that it is one of the few crimes in which the victim is not always very interested in the capture of the criminal. The rather impersonal nature of the majority of these acts diffuses the anger that might otherwise be felt by the apparent victim. The number of hackers in post-communist states is larger than that in the West because there are few adequate laws that might punish them. Moreover once caught and convicted, the criminal enjoys notoriety in criminal circles which enables him to continue his illegal activity once he has served his term. In Russia, the maximum sentence for a computer crime is two years in prison. In terms of career building in Eastern Europe, the convicted hacker should regard his incarceration as time well spent since he is able to make a great deal more money when he resumes his activities.

The Manufacture of False Documents Modern society depends greatly on the acquisition of special skills, education, and training. Certification of those talents is based on the creation of

documents of authentication. Such documents are an absolute necessity in the performance of specialized tasks required for modern society. It is not surprising that there are many people who will provide false documentation for those who want to claim unjustified skills as well as for many others who want to violate the requirements of a technologically advanced society. Nor is it surprising that terrorist organizations place a great deal of emphasis on securing documents – either legitimate or forged - that will help them undermine this society. In fact, one of the responsibilities of the Al Qaeda "finance committee" is to procure passports and entry certificates for the use of its personnel.[21] One of the great ironies is that the availability of modern technology has greatly improved the means for falsification of documents.

Through its "full faith and credit" clause the United States Constitution guarantees that documents produced at the state level must be recognized by other states. This provision, in effect, creates a situation in which fifty state agencies can generate documents that have national validity. The falsification of such documents has long been recognized as a significant problem but our reliance on such documents has greatly increased with the growth and complexity of our social, economic, and legal system. Few forms of identification are more routinely falsified than driver's licenses. This document serves as both a user's permit and an almost universally accepted form of identification. Because each state produces its own version of such a license, authorities are forced to evaluate fifty variations on information to fill basic data sets. For years petty criminals have employed fraudulent driver's licenses in the perpetration of illegal acts. On September 11th, the terrorists responsible for history's most devastating attacks on the United States utilized driver's licenses to identify themselves when they boarded the flight that crashed into the Pentagon.

The terrorist threat has called attention to the vulnerability of all forms of personal documentation. Even more significant ease with which a driver's license may be falsified is the emergence of the increasingly troubling phenomenon known as *identity theft*. Most routine transactions require consumers to use items such as a Social Security number, credit cards, bank account information, or phone numbers. Each of these constitutes a vulnerability that can be exploited with the short-term effect of destroying a person's credit rating, costing him professional opportunities, or

[21] Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press, 2002, p. 68

simply taking up an enormous amount of personal time. The long-term effect, however, is even more significant and may well be the undermining of documentation required for effective operation of economic infrastructure. By 2001, identity theft had become the most common consumer complaint in the United States. The problem has been exacerbated by inadequate legal definitions of what constitutes identity theft, the difficulty of prosecuting cases of identity theft, and restrictions on the utilization of telephonic or hearsay testimonies during preliminary criminal proceedings. [22]

In their utilization of information technology, terrorists have demonstrated an increasingly high level of sophistication. Well educated terrorists now utilize information technology as an important planning tool and an instrument for secure communication. Since the 1990s when Azzam.com was recognized as terrorist web site, the computer has been vital for recruitment. Before 2001, a regular feature of this site was its "Jihad around the world" section which would offer specific locations to which the potential recruit might go in order to meet people. Such sites are also useful for collecting donations from the sympathetic who cannot give up their day jobs to become "jihadists". Hamas, Hizballah, Colombia's FARC, and the Earth Liberation Front host very professional web sites which allow these organizations to define themselves and direct readers to links providing more specific relevant information. Because of the global proliferation of on-line data bases, libraries, and newsgroups terrorists can now turn to the Internet in order to conduct research on targets that may be thousands of miles from their remote training facilities. Finally, this product of an innovative, free society is being employed as an instrument for disseminating terrorist propaganda that can be carefully tailored to meet the interests of very specific groups whose support is needed to enhance terrorist operations. [23]

Summary

The threat identification process has changed dramatically with the rise of new information technologies and the appearance of nihilist threats that are not confined to traditional national boundaries. The effort to identify hostile forces is no longer

[22] "The Rise of Identity Theft in America", *The Daily Cardinal* (University of Wisconsin), December 2, 2002, p. 3

[23] DSCINT Handbook 1.02, *Cyber Operations and Cyber Terrorism*, 15 August 2005, pp. I-1 – I-4.

> confined to those nations seen as our adversaries but must extend into allied states and even our own institutions.
>
> New information technologies have offered new cloaks for those forces bent on the destruction of Western political, social, and economic systems. These easily available instruments have given the widest variety of criminal forces the ability to falsify basic documents and thus undermine the procedures required for effective operation of our basic infrastructures. We can no longer be assured about the validity of passports, driver's licenses, university diplomas, or any of the instruments essential for establishing personal identities. Terrorist organizations can now create impenetrable personal histories that enable them to elude many of the best efforts of the law enforcement community.
>
> An especially devastating impact of new information technologies is that criminals routinely invade Western commercial and governmental networks. Untold billions of dollars have been spirited out of institutions once deemed invulnerable. The routes taken by those funds all too often coincide with the transit centers for weapons being directed into the hands of violent terrorist organizations. At the same time, American universities, as bastions of free inquiry, now provide opportunities for terrorists agents determined to legally acquire technical skills that can be used to undermine the society that created these important educational opportunities.

You are left with the awesome responsibility / need for international cooperation. If this threat is transnational then the response must be international or the response will never be successful. Yet America cannot get NATO, the most stable and long standing of international coalitions to agree on the threat.

Danish cartoon – can finally get artists to agree on the threat. When will nation states agree?

The diplomatic arm of our nation (which cannot even get its own foreign service officers to deploy to hostile areas) must engage other nations to both protect our nation and to defeat this transnational threat.

Authors

Stephen R. Bowers is a Professor of Government in the Helms School of Government at Liberty University and Director of the Center for Security and Science. He is a graduate of the University of Tennessee and a retired US Army Lieutenant Colonel who worked in the area of special operations. He is the author of *Technology and Terrorism* which was published by the London-based Center for the Study of Conflict and Terrorism in 1998 as well as numerous publications on political violence in the former USSR.

Stephen M. Parke is Associate Dean, Helms School of Government and an Assistant Professor of Criminal Justice. Professor Parke retired from the United States Army in August of 2006 following 21 years as a supervisory Staff Judge Advocate. His positions in the U. S Army culminated with his selection as the Staff Judge Advocate for Joint Task Force – Guantanamo. Professor Parke holds B.S., J.D., and L.L.M. degrees.