2006

Digital Repertoires: Non-State Actors and ICTs

Christopher J. Cox
University of North Florida

Digital Repertoires: Non-State Actors and ICTs

Christopher J. Cox

Faculty Sponsor: Paul G. Harwood,
Assistant Professor of Political Science

Abstract

In this paper we explore the usage of information communication technologies (ICTs) in the proliferation of non-state political violence, and governmental countermeasures to thwart such actions. We are specifically interested in gauging how communication technologies are being adapted to provide such non-state with new terrorist repertoires. To explore this issue, we utilize personal interviews with members of the U.S. government and members of Washington's IT security community.

Introduction

In 1993, when the World Trade Center was bombed, there were 130 websites (Irving 1998; Surratt 2001; Smithsonian 2003). [1] By September 2001, there were well in excess of a billion, with an estimated seven million pages being uploaded daily (Castells 2001; Introna and Nissenbaum, 2000). In 1993, 22 articles about the Internet appeared in the *New York Times* (New York Times, 1994).[2] In 2001, between October and December alone, better than 760 Internet stories were deemed "all the news that's fit to print" (New York Times, 2002). In 1993, some 13 million Americans had cell phones, by 2001 there were 180 million subscribers (McFarland 2002; Tesar 1983.) Today, American electoral politics is online, with candidates for county commissioner to the Presidency advertising via glossy websites (Bonchek 1997; Davis 1999; Anderson and Cornfield 2003; Levine 2003; Norris 2001; Rash 1997). Moreover, economics has gone digital, with U.S. online retail spending, *e-commerce*, worth forty-five billion dollars in 2002, and high-tech industries driving about one-quarter of all economic growth.[3] These figures reveal an incredible technological and behavioral phenomenon. Information communication technologies (ICTs) are therefore "the instruments with which and the conditions within which we enact some of the most profound conduct of lives" (Fischer 1992, 7). By any measure, computer-mediated communication (CMC) and "new" ICTs are embedded within the fabric of daily life — the way we shop, do business, obtain information, and communicate with others. These new technological appliances, or more precisely their *usage*, have changed society.

Clearly, "[s]cience and technology have made enormous progress, but human nature, alas has not changed" (Laqueur 1999, 4). Thus, while ICTs are applied for positive goals, such as maintaining social relationships across

[1] There were 130 websites in June 1993 (Surratt 2001; Irving 1998). There are no available statistics for February 1993. By the end of 1993, there were 623 websites (Irving 1998; Smithsonian 2003).

[2] In 1992, there were only two stories about the Internet in the *New York Times* (See New York Times Index, vol.80).

[3] The figure of $45 billion does not include online travel or other ticket sales, nor monies spent through online brokerages (Regan 2003).

vast distances, they have a darker side, where their adaptation has met the sinister needs of our human nature, such as crime,[4] and as discussed in this paper, terrorist violence by non-state political actors. "The idea of terrorists surreptiously hacking into a computer system to introduce a virus, steal sensitive information, deface or swamp a web site, or turn off a crucial public service seriously concerns security personnel around the world" (Zanini and Edwards 2001, 29; see also Arquilla and Ronfeldt 2001).

Utilizing personal interviews of members of the U.S. government and Washington's IT security community, this paper examines the adoption and adaptation of ICTs in the proliferation of non-state political violence and the governmental countermeasures to thwart such actions. First, we specifically gauge how communication technologies are being adapted to provide non-state actors with new terrorist repertoires (Tarrow 1998). Here, accepting Enders and Sandler's (2002) definition of terrorism, we examine how ICT repertoires emerge and spread, concluding that the usage of "traditional" ICTs, technologies which have achieved critical mass, dominate the terrorist's ICT toolbox and are utilized to meet organizational needs (Morris and Ogan 1996; Tarrow 1998; Arquilla and Ronfeldt 2001). Second, recognizing that terrorism does not occur in a vacuum, we explore the counterterrorism measures being employed by the U.S. government to fight non-state political violence, finding that new countermeasures by governments are, in part, dependent on the availability of new technologies. Moreover, we find a commitment to a macro-level approach to adopting passive countermeasures, in order to combat the organizational functions ICTs perform for nonstate terrorists, while avoiding the pitfalls of piecemeal policy efforts of the past in the physical prevention of terrorist entering the United States (see Enders and Sanders 1993).

[4] For example, since 2003, credit card fraud and identity theft, have been among America's fastest growing crimes. For example, 43% of fraud cases filed with the Federal Trade Commission (FTC) were identity theft complaints, making it the number one complaint in 2002 (Federal Trade Commission, 2003).

Terrorism

"Mr. President, we are under attack"
Andrew Card, Chief of Staff to President George W. Bush, September 11th, 2001.

On September 11th, 2001, eight times as many people died in the space of an hour to transnational terrorism than during an average year (see Enders and Sanders 2002, 145). Today, transnational terrorism –"when an incident is planned in one country but executed in another"- provides a threat to U.S. democracy and our domestic tranquility, even though historically such terrorism has only directly affected relatively few people (Laqueur 1999, 4). The atrocities of 9-11 shocked Americans and have engaged the American government in the largest national security initiative since World War II.

Terrorism is not easy to define. In this paper, however, we accept Ender's and Sandler's (2002) definition of terrorism. "Terrorism is the premeditated use or threat of extra normal violence or brutality by sub national groups to obtain a political, religious, or ideological objective through intimidation of a huge audience, usually not directly with the policy making that the terrorists seek to influence" (2002 146). This definition has broad applicability, and allows for

variations in the scope of repertoires and organization of terrorist entities- state and nonstate actors. In policymaking circles, where all politics is local, definitions of terrorism embody patriotism.

> "Ah, I think the more you look at terrorism, and try and understand the problem of terrorism, the more you realize, ah, its, politics, politics is always going to play a role in the definition of terrorism. …Senator Graham has generally tried to take a more pragmatic approach, umm, and just identify, is this group that wants to harm Americans? And ah, if it is, them, ah, we should treat them as terrorists" (Dickas, 2004).

While these two definitions differ in application and understanding, the two are equally salient, illustrating academic and policymaking realities.

There are three main precepts in the identification and classification of a terrorist act. A terrorist action has three elements to it — target, devastation goal, and tool (For examples of earlier typologies see Drake 1998). Targets can vary from civilian institutions (shopping malls) and transportation (airplanes and ocean liners), to military installations and armaments (ships and aircraft) (Laqueur 1999; Stern 1999). The terrorist's tool of choice can vary too, from small explosives to civilian airliners used as flying bombs. Devastation goal refers to the level and significance of damage, whether physical or psychological, that a terrorist group seeks in their actions (Reich 1990; Crenshaw 2000). In this paper we focus on the latter — the tool — notably the usage of information technology, and especially ICTs that have achieved critical mass.

Historically, terrorism has been used as the tool of separatists, zealots, and patriots in an ultimate attempt to spawn social change, political upheaval, and revolution. Acts of violence by non-state actors pre-dates thee 14th century; it is not until the late 18th century that the word "terrorism" is spawned. The trouble with terrorism is not that it has always been indefensible but that it has been chosen more often than not as the prima ratio of self-appointed saviors of freedom and justice, of fanatics and madmen, not as the ultimate ratio of rebels against real tyranny (Laqueur 1999, 10).

The word *terrorism* originated in 1795, in connection with the French revolutionaries who executed their enemies and surpressed opposition with the guillotine (Crenshaw 1990, 10). The concept of terrorism took greater hold during the 1870s in Russia, when revolutionaries began to practise it. It was a means for weaker or smaller forces, without the financial means or military strength of larger countries, to wage war, essentially the only option for those unable to fight an orthodox struggle. Soon, the tactic spread to the Macedonians and Armenians of the Ottoman Empire, the Irish and the Indians in the British Empire, and separatists in America and Europe (Enders and Sanders 1993). In the twentieth century, terrorism would come from both sides of the political spectrum, first from the left and then in the mid 1970s and later, from the right, most notably in Europe. Terrorism, a nuisance to the many, has had a long history (Laqueur 1999, 4-5). Biblical martyrs, Roman dissidents, French révolutionnaire's, and English turncoats all serve to establish the history of terrorism. Thus, while we do not compare the acts of Al Qaeda and the like to the

American founders, the principle and the three elements remain comparable. Terrorism has overthrown dictators, toppled monarchs, and dispelled tyrants throughout the ages, and will continue to serve those who seek its ubiquitous assistance.

Understanding terrorism generally is impossible if the logic behind the decision to commit acts of terror is unapparent. Terrorists are rational actors (Crenshaw 1990: 2000; Zanini and Edwards, 2001). The actions of terrorists serve as the avenues of communication, and are generally motivated by a desire to gain public attention and media coverage. Most often than not terrorist actors feel that all areas of communication and compromise are exhausted. Terrorism is seen, therefore, as the best, if not the only, avenue open to them.

Terrorism may in fact follow logical processes that can be discovered and explained. For the purpose of presenting this source of terrorist behavior, rather than the psychological one, it interprets the resort to violence as a willful choice made by an organization for political and strategic reasons, rather than as the unintended outcome of psychological or social factors (Crenshaw 2000, 7-8). It is important to recognize the political psychology behind terrorist actions since it enables one to fully analyze terrorist action and determine why the act was committed, by whom, and what future action may be expected.

So what is the current state of affairs? The War on Terror that began when America was attacked, has involved billions of dollars in America alone, and defense spending is still on the rise. The creation of the Department of Homeland Security (DHS) in 2002 represented one of the largest governmental restructuring in history. With its broad executive power, and an enormous annual budget, the DHS serves as the supreme authority in domestic protection. Post 9/11 the real question in the back of the minds of Americans is very simple; “Is America safer today than it was on September 10, 2001?”

This, like defining terrorism, is not easily answered. John Dickas (2004), head of terrorism for former Senator Bob Graham of Florida spoke to this;

> Ah, [pause], No. Well, [pause] I think in terms of, I don’t think the threat is diminished, I think, we have improved our security precautions in a lot of ways, especially aviation security.

Speaking from a policymaking and political standpoint, many see homeland security as a multi dimensional, multi-faceted operation, where large targets are emphasized, and security is maintained in the public domain. While certain potential areas of terrorist penetration have become much more secure; aviation, immigration, and event security, plenty of areas of weakness can be found.

If we are to learn anything from the September 11 attacks it is that terrorist groups use well planned and unsuspecting means to launch their large scale attacks. The necessity of media coverage coupled with the media and public’s tendency to become inured to a certain level of death and destruction motivates terrorist organizations to be innovative and to collaborate with other groups to learn and develop new ways to kill and destroy. (Arquilla & Ronfeldt 1999; Bell 1984; Bassiouni 1982; Edelman 1988; Crigler 1996; Katz and Lazarsfeld 1955; Martin 1985; Podhoretz 1981; Zaller 1992). Areas of weakness as

well as recent technological advancements have served to make the terrorist threat much more complex and harder to detect and defend. “In the near future it will be technologically possible to kill thousands, perhaps hundreds of thousands, not to mention the toll the panic that is likely to ensue may take” (Laqueur 1999, 4). The availability of weapons of mass destruction also has policymakers and defense analysts worried. If terrorists gain control of such a device, the devastation would be catastrophic. These new mediums and tools pose a greater threat to society now than in the past, largely because of the new methods that terrorists now have available. While science has allowed for great advancements in technology, human nature has not changed. Those who wish to cause harm now have a new frontier upon which to stage, conduct, and execute their attacks, thus challenging the world to a new type of war.

Repertoires

Before analyzing the role of ICTs in terrorism, we need to theoretically situate our analytical approach. Research on terrorist repertories has pointed at terrorist motivations, resources, and media attention as leading causes of weapon choice (Morris and Hoe 1980 80-86; Paletz el al.1982; Schaffert 1992). In this paper, we also draw from the literature of social movements, civil conflict and war; notably, Tarrow’s (1994) work on political opportunity structures. In *Power of Movements* (1994, 19), Tarrow points out that political action by groups does not just pop out of the heads of organizers but is part of what he calls a “repertoire of contention” which forms a tool kit that a group can draw from to try and get its message across. Thus, we ask, what ICTs do non-state terrorist actors have within their respective toolkits? And, how do they use them?

ICTs and Terrorism

Information communication technologies (ICTs), or our use of them, as stated, have changed the way we live our lives, and their darker side, is “altering the nature of conflict across the spectrum” (Arquilla and Ronfeldt 2001, 1). The adoption of new ICTs, notably Internet appliances (chat rooms, bulletin boards, and email) and cell phones, by nonstate terrorists is organizationally advantageous (Gehrett 2004). With geographically dispersed constituents, who increasingly are carrying out distinct, yet corresponding activities, bi- and multidirectional ICTs are able to facilitate the quick dissemination of information across a decentralized terrorist network (Arquilla and Ronfeldt 2001,1: see also Enders and Sanders 2002). Such ICTs are new additional tools within a terrorist group’s repertoire that are being utilized to meet the organizational needs of decentralized networks. In addition, it is important to note that, information-age technology can help terrorists conduct three broad types of offensive information operations (IO). First, it can aid them in their perception management and propaganda activities. Next, such technology can be used to attack virtual targets for disruptive purposes. Finally, IT can be used to cause physical destruction (Zanini and Edwards 2001, 41). From our interviews, however, we find the greatest concern among Washington insiders’ centers around the organizational functions everyday ICTs, such as the Internet, are providing

terrorists. Arquilla and Ronfeldt's (2001, 1) concept of "netwar," even in our post 9-11 world, is pertinent. It is this subject therefore, that dominates our discussion.

Succinctly, the importance of ICTs today to nonstate terrorists is first and foremost their ability to facilitate organization, the central tenet of Arquilla and Ronfeldt's (2001) concept of netwar. Netwar is a result of the rise of network forms of organization, which in turn is partly a result of the computerized information revolution. To realize its potential, a fully interconnected network requires a capacity for constant, dense information and communication flows, more so than do other forms of organization (e.g., hierarchies). This capacity is afforded by the latest information and communication technologies- cellular telephones, fax machines, electronic mail (email), web sites, and computer conferencing (Arquilla and Ronfeldt 2001, 10).

Terrorists are adopting and using ICTs for more than the dissemination of spoken or written information though. A significant component of the organizational dynamic within netwar is financial (Dickas 2004; Platt 2004). Many of binary ones and zeros that have interested US intelligence since 9-11 have centered on electronic funds transfers within bin Laden's Al-Qaeda network (Dickas 2004; Gehrett 2004; Hutchinson 2004).

So what makes a nonstate terrorist select an ICT? There are a number of reasons, but the selection process is, in part, based on a particular ICTs cost effectiveness. The introduction of new technologies in an organization follows a complex and often lengthy process. Not only do innovative systems have to be developed or acquired, but organizational actors have to become familiar with new systems and be able to use them effectively. Given the challenge, terrorist groups are likely to channel their scarce organizational resources to acquire those IT skills that have the greatest leverage for the least amount of cost and effort (Zanini and Edwards 2001, 50).
It is not surprising, therefore, that terrorists are using readily available technologies that are entrenched within the fabric of industrial societies. The embeddedness of the technologies used makes communications, as will be discussed later with regard to counterterrorism, via them difficult to control, although not impossible to intercept.

Thus, we argue it is useful to see the usage of ICTs by terrorist nonstate actors, as social constructivism, rather than technological determinism. The terrorist organization is "neither impacted by an external force, nor are they the unconscious pawns of cultural *Geist*. Instead of being manipulated, [it] manipulates (Fischer 1992, 17). Technologies are not repressively foisted upon passive populations, any more than the power to realize their repressive potential is in the hands of a conspiring few. They are developed at any one time and place in accord with a complex set of existing rules or rational procedures, institutional histories, technical possibilities, and last, but not least, popular desires (Penley and Ross, 1991).

Equally essential, different ICTs will be applied for separate goals. As Claude Fischer (1992, 7) notes, "separable parts of a technological system may have separable consequences." Thus, a terrorist may use the Internet's separable parts, such as email and chat-rooms, differently to achieve different goals. As Zanini and Edwards note, Bin-Laden's "operatives

have used CD-ROM disks to store and disseminate information on recruiting, bomb-making," and "Hamas activists in the United States use chat rooms to plan operations" (Zanini and Edwards 2001, 37). In short, different ICTs have different uses.

Nonstate actors adopt pre-existing technologies. They are not involved in technological innovation, rather mere technological adaptation. The ICTs used by terrorists are not the latest groundbreaking advances in technology, but rather commercial technologies which have already been broadly adopted in Western societies. Moreover, in communication theory terms, the ICTs of choice for nonstate terrorists have achieved *critical mass*, which is "when about 10-20 percent of the population has adopted a news innovation, the innovation can be spread to the rest of the social system" (Morris & Ogan 1996: 45). Recognition of the theory of critical mass helps explain further the cost effectiveness component of ICTs choice by terrorists.

Not only are the ICTs adopted established technologies in industrial states, but these new tools are not replacing older, or non-technological, tools within a terrorists repertoire of contention. Rather, what we conclude is while ICTs are facilitators of the day-to-day organizational networking of a group, "electronically mediated coordination will not be able to entirely supplant face-to-face exchanges" between network members. The supposed anonymity ICTs, such as chat-rooms and bulletin boards provide, does not allow for trust to be built between constituent members. Human face-to-face interaction, as the civil society and social networks literature indicates, is important to foster trust (Harwood and McIntosh 2004; Kraut et al. 1998; Kraut et al. 2001). "Human couriers and face-to face meetings may still remain essential" for terrorists (Arquilla and Ronfeldt 2001, 339).

The combining of old and new is also a product of "communication over electronic channels can become a liability, since it leaves digital traces" (Zanini and Edwards 2001, 39). Mistrust, therefore, also centers on the level of anonymity new ICTs, such as the Internet and cellular phones provide. This mistrust is justified since "Carnivore's ability to track Osama bin Laden's email was critical in thwarting several of his strikes" (Zanini and Edwards 2001, 39). Thus, the adoption of technologies by nonstate terrorist actors is a complex decision. They are not just adopted and adapted because the technology is there. "There is no built-in demand to innovate" for terrorists. Netwar, therefore, as Arquilla and Ronfeldt (2001, 339) state, "can be waged without necessarily having access to the Internet and other advanced technologies. This level may mix old and new, low-and high-tech capabilities." New technologies, therefore, are not necessarily replacing old methods or tools within terrorists' toolbox (Tarrow 1998).

The question for today and tomorrow is whether terrorists have the desire and opportunity to significantly increase their reliance on IT, not for organizational means, but to achieve disruptive and destructive IO? Is the usage of cell-phones as detonation devices, as occurred in Madrid last year, only the beginning? While a concern voiced by several academics, notably Arquilla and Ronfeldt, from our interviews, we find little concern for the emergence of newer, more

technologically savvy groups (Gehrett 2004; Hutchinson 2004; Platt 2004). Instead, we find counterterrorism efforts focusing on overcoming the organizational usage of ICTs, as well as, the physical prevention of terrorists into the United States.

Countermeasures against Terrorism

Terrorism does not occur in a vacuum. Counterterrorism efforts to detect, prevent, and/or mitigate damage, destruction, or death from a particular terrorist repertoire, operate simultaneously with terrorism. In the post 9-11 world, the nonstate terrorist is a multi-organizational decentralized network that presents structural problems for industrial intelligence organizations to overcome. Government bureaucracies are hierarchical structures that closely guard their policy turf. Such structures do not serve contemporary counterterrorism efforts well. As Arquilla and Ronfeldt (2001, 15) note, "[i]t takes networks to fight networks." Decentralized bureaucracies, such as the idea behind the Department of Homeland Security are necessary to more effectively morph terrorist group structures.[5] Destroying terrorist organizations' organizational structure is key to preventing offensive attacks, and for keeping America safe. Policymaking cannot, therefore, be piecemeal since in the past, such efforts were ineffective (Enders and Sanders 1993). In short, counterterrorism must be all encompassing, incorporating both active and passive policies, and have micro- and macro-level strategies, while remaining protective of the civil rights of citizens (Hutchinson 2004). This is not an easy task.

At the macro-level, the question is, how should authorities stop attacks using national-level efforts to thwart entry of "bad actors" and weaponry? Enders & Sandler (1993) and Landes (1978) concentrate primarily (but not solely) on broad-based countermeasures that target no particular repertoire. The Department of Homeland Security's strategic plan (U.S. Department of Homeland Security, 2004, 14) in Objectives 2 and 3, speaks to this by focusing primarily on efforts to "interdict…unlawful migration of people, cargo, drugs, and other contraband," protect infrastructure from generic forms of attack, and assure broad-based sharing of knowledge. These examples of macro-management serve to provide the overarching infrastructure of counterterrorism.

At the micro level, countermeasures target a specific terrorist repertoire, seeking to develop combatant strategies that are both effective and feasible. Examples of micro level management can be seen with the reaction of the United States against the terror attacks of September 11. The usage of hijacked airplanes to propagate terrorism was not a new phenomenon, it was how Al Qaeda operatives gained control, and further used the airplanes, which was the new repertoire. The United States responded simultaneously on the micro and macro level policies. On the macro level, as stated above, was the creation on the Department of Homeland Security and the establishment of the Transportation Security Agency. On the micro level, America witnessed the installation of advanced screening

[5] The idea is only the first step. Implementation is key. We find certain dissatisfaction from democrats, for example, Senator Nelson of Florida, on the implementation. "Ah, he supported the idea, but has been disappointed by the implementation" of the Department of Homeland Security (Platt 2004).

equipment and personnel at all airports, the commissioning of air marshals, and the prohibition of carry on items any of which could pose a possible risk. Along with such passive policies we also witnessed active policies, most notably "taking out a lot of terrorist training camps in Afghanistan" (Platt 2004). It is important, therefore, to recognize both levels of strategy have a job to do, counteracting individual repertoires on the micro level and instituting appropriate policy on the macro level.

Technology undeniably has a role to play in counterterrorism. The technology is non-traditional, i.e., the latest advancements in IT. These devices, both active and passive, offer unprecedented new capabilities that will, it is hoped, save lives and keep Americans at home and abroad safer. The commitment and role of technological advances in the War on Terror is evident from the allocations for defense spending on R&D in 2005. This year such spending will increase by 6.8 percent or $4.8 billion to another all-time high.

From interviews with members of the U.S. government and IT security community, the following are implemented or forthcoming governmentally initiated programs that are utilizing information technologies to safeguard America.

First, is nanotechnology. While politicians, with the exception of Asa Hutchinson, did not speak to this, Ann Gehrett of CACI was particularly enthusiastic about the potential nanotechnology heralds for counterterrorism. Nanotechnology is still in the very early stages of its R&D, but the basis of nanotechnology revolves around the application of science in the development of new materials and processes through the manipulation of molecular and atomic particles.

Second, there was much discussion among both politicians and IT security specialists about biometrics. Biometric technologies automatically authenticate, identify, or verify an individual based on physiological or behavioral characteristics. This process is accomplished by using computer technology in a non-invasive way to match patterns of live individuals in real time against enrolled records. Examples include products that recognize faces, hands, fingers, signatures, irises, voices, and fingerprints. Biometrics is currently being used to enhance computer network security, protect financial transactions, regulate immigration, and monitor border flow (Dornbush 2005). Currently the Department of Homeland Security is using biometrics in conjunction with terrorist watch lists and databases in the US-VISIT system. The US-VISIT system links databases to provide valuable information to port of entry officials and consular officials overseas and creates a database of pictures and finger scans of everyone entering the United States with a non-immigrant visa (and soon to include visa waiver travelers). This new tool means that we have a much better idea of who is entering our country. If an individual's finger scan registers a match on the terrorist watch list, the Department is able to stop them from entering the country at the border. Over 200 people have already been turned away from our borders using this new system (DHS Fact Sheet, 2004). The benefits of biometrics are not only its ability to be a stand-alone safeguard, but it is also well suited to work in conjunction with other technologies to create a multi-layered security infrastructure.

Third, there was some discussion, notably by Asa Hutchinson, Under-Secretary of Homeland Security, and Ann Gehrett of CACI, about BioWatch, which is a series of environmental monitors located in various cities throughout the U.S. These monitors provide an early warning of a potential chemical or biological attack, allowing for immediate countermeasures and treatment. The Department of Homeland Security is also deploying and evaluating mobile automatic air testing kits that house biological and chemical sensors allowing for instantaneous detection anywhere. As well as BioWatch, they discussed BioShield which is an aggressive campaign that seeks to develop and maintain medical vaccines and supplies that would be deployed and administered in the event of an attack (DHS Fact Sheet, 2004). BioWatch coupled with Bioshield, they suggested comprising safeguard that serves to keep America's cities and their citizens' safe before, during, and after an attack.

Fourth and while not involving advanced technologies on the scale of nanotechnology, but equally important to a macro/micro-level strategy, is the integration of federal and state computer databases. Just as hierarchical bureaucracies provide a pitfall for fighting non-state terrorism, so too does federalism. Timely and accurate exchange of information between the federal, state, and local governments is crucial in the prevention, detection, and arrest of terrorists and terrorist activities. Post September 11, the information sharing abilities of U.S. law enforcement and intelligence remained poor; "we have a lot of problems with information sharing, ah, works being done that's redundant, or ah, or works being pursued on parallel tracks with no communications, we have a lot of problems of that nature" (Dickas, 2004). It is particularly poor at the local level, with both of Florida's Senators spokespersons noting there is a "need for more information-sharing" particularly in the dissemination of "timely information" to local agencies (Dickas 2004: Platt 2004). "I know the higher up you get, the better it gets, but it never gets very good" (Platt 2004).

While Senator Gramm's spokesperson suggests more needs to be done, several policies are in the field. The recent creation of The Homeland Security Information Network, which is available in all 50 states, makes threat-related information available to law enforcement and emergency managers on a daily basis through a web-based system (Hutchinson 2004). In addition, members of 35 different Federal agencies are now all co-located together in the DHS's new 24-hour Homeland Security Operations Center, which allows the information coming from various sources to be synthesized together and then shared with other federal partners such as the FBI and the Department of Defense. Furthermore, nearly 100 bulletins and other threat related dossiers have been sent to homeland security professionals across the country (DHS Fact Sheet, 2004).

While no one we interviewed spoke to this, it is also important to note that integration cross nationally must occur also. "There is," as Enders and Sanders (2002) note, "an irony, because collective action among terrorist groups in sharing training and financing has been quite substantial. To date, this suggests that terrorists are more united in their common goals than are countries in addressing the transnational terrorist threat." The lack of discussion of this issue may be, in part, a product of the

national-centric definition of terrorism used by policymakers (Dickas 2004); however, if a macro-level strategy is to be effective, a global component must feature, particularly in passive policies of data and information-sharing.

Lastly, several interviewees spoke of Operation Liberty Shield. This program truly embodies protecting the homeland as in conjunction with the federal government, many private sector companies work to ensure American remains safe. Although the two share a common goal, the private sector often takes a different approach to homeland security. CACI is one example of a private corporation whose primary objective is working with the federal government to ensure homeland security. Operation Liberty Shield is a program that displays this collective action. Operation Liberty Shield is a "comprehensive national plan designed to increase protections for America's citizens and infrastructure while maintaining the free flow of goods and people across our border with minimal disruption to our economy and way of life" (CACI, 2005). Operation Liberty Shield incorporates various different governmental agencies, and is critical in the protection of American domestic security and surveillance. Anne Gehrett, CACI's vice-president for law enforcement programs, particularly emphasized throughout the interview the importance of this multi-agency cooperation, primarily through the dissemination of information, and the intensive usage of terrorist watch lists and databases (Gehrett, 2004).

All of these countermeasures, to varying degrees involve ICTs, and together formulate core components in America's fight against terrorism. While these technologies and programs serve to keep Americans safer, they are but just the initial phase (Hutchinson 2004). Much still needs to be done. Great emphasis has been placed on the homeland since 9/11, however what about American interests abroad? It is overseas after all, that Americans are most are risk (Enders and Sanders 2002, 162). The sharing of information amongst governments, as we suggest, while a step in the right direction, is currently flawed since no formal anti-terrorism campaign has been established on an international scale, thus information sharing between international agencies and state actors is piecemeal, which will prove ineffective.

Today, terrorism is limitless in its geographical scope. It fails to adhere to recognizable borders, and discerns no international set of laws. The two types of analysis serve to combat terrorism in two very different ways, and their application can mean the difference in the success or failure of the terrorist act. Speaking in terms of macro application little can be done legislatively to protect the individual. Many of the millions spent on macro applications of legislature only result in the diminishing of personal freedoms, a sort of societal nuisances. Micro level application targets individual repertoires of the terrorist threat, thereby targeting terrorism with a personalized strategy. While it is easy to say what would work in theory, it must remain salient that terrorism will always remain a threat to those it seeks to target. In the end, the most effective weapon against the terrorist threat remains as basic today as it will a decade from now; keen awareness of any possible threat, preparation for any attack, and responding immediately to any emergency.

Conclusion

In conclusion, we find two very different ICT stories being told. First, there is the story of non-state terrorists. This is a tale in which traditional ICTs, mediums that have achieved critical mass, are being used to further, and maintain, a group's decentralized, multi-organizational, network. Here, ICTs play a supporting role, since netwar, at its core, is about organization (Arquilla and Ronfeldt 2001). The usage of traditional ICTs by non-state terrorist actors is to facilitate information-sharing and knowledge. Furthermore, we find traditional ICTs are clearly additional tools within the terrorist's toolbox. The adoption of new ICTs, therefore, does not replace, by rather supplement, pre-existing tools, notably face-to-face meetings and human couriers. Lastly, we find the concerns expressed in several academic works of the potential for new high-tech terrorists groups (Laqueur 1999; Arquilla and Ronfeldt 2001) is not voiced by our interviewees whose concerns rather center on the organizational role ICTs play in terrorism today. This disparity of concern among academics and practitioners we hope to explore in future research.

Turning to counterterrorism, a very different story is told. Here, the latest technological advancements are being utilized to combat terrorism. Biometrics, as Asa Hutchinson (2004) noted for example, has allowed for unprecedented steps to be taken in the protection of key areas of infrastructure, thereby limiting potential terrorist targets. In addition, the integration of databases and watch lists is furthering information sharing efforts throughout the federal system. From our interviews, it is evident that effective counterterrorism will continue to incorporate active and passive policies at both the micro and macro levels.

While technology will continue to advance, human nature will remain unchanged. Terrorism has always been apart of American history; it didn't begin on September 11, 2001. Combating terrorism today is an incredibly salient policy issue, with billions spent already, and billions more still to come. As John Dickas acknowledges, the "threat is diminished," however, much remains to be done to ensure a secure America from terrorism by nonstate political actors.

References

American Association for the Advancement of Science (AAAS). 2004. "Defense and Homeland Security R&D Hit New Highs in 2005; Growth Slows for Other Agencies." AAAS, November, 2004. <http://www.aaas.org/spp/rd/upd1104.htm>. (Date visited January 15, 2005).

Anderson, David and Michael Cornfield. eds. *The Civic Web: Online Politics and Democratic Values.* Lanham, MD: Rowman and Littlefield Publishers, Inc., 2003.

Arquilla, John and David Ronfeldt. "The Advent of Netwar." *Networks and* Netwars. Arquilla, John and David Ronfeldt. Ed. RAND: Santa Monica 2001.

Arquilla, John and David Ronfeldt. "What Next For Networks and Netwars?" *Networks and Netwars*. Arquilla, John and David Ronfeldt. Ed. RAND: Santa Monica 2001.

Bassiouni, M.C. (1982). Media Coverage of Terrorism. *Journal of Communication 32*, 128-143.

Bell, J. (1974). Terrorist Scripts and Live Action Spectaculars. *Columbia Journalism Review 17*, 47-50.

Bonchek, Michael. "From Broadcast to Netcast," 1997. <http://www.ai.mit.edu/msb/thesis> (Date visited: 29 December 2004).

CACI (2005) <http://www.caci.com/hls.shtml> (Date visited: 15 January 2005).

Castells, Manuel. *The Internet Galaxy: Reflections on the Internet, Business and Society*. Oxford: Oxford University Press 2001.

Crenshaw, M. (2000). "The Psychology of Terrorism: An Agenda for the 21st Century" *Political Psychology 21*(2).

Crigler, A. (Ed.). (1996). *The Psychology of Political Communication.* Ann Arbor: University of Michigan Press.

Davis, Richard. *The Web of Politics*. Oxford: Oxford University Press, 1999.

Department of Homeland Security 2005 "Threats and Protection." <http://www.dhs.gov/dhspublic/theme_home6.jsp> (Date visited: 02 February 2005).

Dickas, John, Special Assistant: Office of Senator Bob Graham. Personal Interview, July 2004.

Dornbush, Rebecca. *Biometrics – The State of the Art*. <http://www.biometrics.co.za/tech_Dorbush.htm> (Date visited: 08 January 2005).

Drake, C.J.M. (1998). *Terrorists' Target Selection*. Houndmills, Basingstoke, Hampshire; New York: Macmillan Press; St. Martin's Press.

Edelman, M. (1988). *Constructing a Political Spectacle*. Chicago: The University of Chicago Press.

Enders, W., & Sandler, T. (1993). The Effectiveness of Anti-Terrorism Policies: Vector Autoregression-Intervention Analysis. *American Political Science Review*, *87*(4), 829-844.

Enders, Walter, and Todd Sandler (2002). Patterns of Transnational Terrorism, 1970–1999: Alternative Time-Series Estimates. *International Studies Quarterly 46*(2), 145.

Fischer, Claude *America Calling: A Social History of the Telephone to 1940.* Berkeley: University of California Press, 1992a.

Gehrett, Anne, Vice-President of Law Enforcement Program, CACI. Personal Interview, July 2004.

Harwood, Paul and Wayne McIntosh. "Virtual Distance and America's Changing Sense of Community." *Democracy Online*. Peter Shane, Ed. London: Routledge 2004.

Hutchinson, Asa, Under Secretary for Border & Transportation Security, Personal Interview, July 2004.

Introna, Lucas and Helen Nissenbaum. 2000. "Shaping the Web: Why the Politics of Search Engines Matter." The Information Society. Vol. 16, no.3 (2000). 169-186. <http://www.slis.indiana.edu/TIS/articles/introna163.htm> (Date visited January 23, 2002).

Irving, Larry. "The Next Waves In Wireless Technologies"1998. <http://www.ntia.doc.gov/ntiahome/speeches/rawcon.htm> (Date visited: March 2nd, 2003).

Katz, E and P. Lazarsfeld. (1955). *Personal Influence*: *The Part Played by People in the Flow of Mass Communicatio*. Glencoe, Ill.: Free Press.

Keck, Margaret and Kathryn Sikkink 1998. *Activists Beyond Borders: Advocacy Networks in International Politics*. Ithaca, NY: Cornell University Press.

Kraut, Robert, Vicki Lundmark, Michael Patterson, Sara Kiesler, Tridas Mukopadhyay, and William Scherlis. "Internet Paradox: A Social Technology That Reduces Social Involvement and Psychological Well-Being?" *American Psychologist*. 53.9 (1998): 1017-1031. <http://www.apa.org/journals/amp/amp5391017.html> (Date visited: 1 October 2000).

Kraut, Robert, Sara Kiesler, Bonka Boneva, Jonathon Cummings, Vicki Helgeson and Ann Crawford. "Internet Paradox Revisited." *Journal of Social* Issues. 2001.

Landes, W. M. (1978). An Economic Study of US Aircraft Hijackings, 1961, 1976. *Journal of Law and Economics, 21*, 1-31.

Laqueur, Walter. (1999). *The New Terrorism*: *Fanaticism and the Arms of Mass Destruction.* New York: Oxford University Press.

Levine, Peter. "The Internet and Civil Society." Unpublished Manuscript. 2001.

Martin, L.J. (1985). The Media's Role in International Terrorism. *Terrorism 8*, 44, 58.

McFarland, Deidre. Cell Phone Ownership Grows 29 Percent from 1999-2001. Scarborough Research. March 18, 2002.

Morris, Eric and Alan Hoe. (1980). *Terrorism*: *Threat and Response*. New York: St. Martin's Press.

Morris, Merill and Christine Ogan. "The Internet As Mass Medium." *Journal of Communication* 46.1 (1996): 39-50.

New York Times, *The New York Times Index1992*. v.80. New York: The New York Times Co. 1993.

New York Times, *The New York Times Index 1993*, v.81. New York: The New York Times Co.1994.

New York Times, *The New York Times Quarterly Accumulation*, January-March, 2002.

Norris, Pippa. *Digital Divide*: *Civic Engagement, Information Poverty, and the Internet* Worldwide. Cambridge: Cambridge University Press, 2001.

Paletz, D, Ayanian, J & P. Fozzard(1982). “Terrorism on Television News: The IRA, the FALN, and the Red Brigades.” In W. Adams (Ed). *Television Coverage of International* Affairs. Norwood, NJ: Ablex.

Penley, Constance and Andrew Ross. *Technoculture.* Minneapolis, Minn: The University of Minnesota, 1991.

Platt, Katie. Special Assistant, Office of Senator Bill Nelson. Personal Interview, July 2004.

Podhoretz, N (1981).The Subtle Collusion. *Political Communication and Persuasion 1*, 84-89.

Rash, Wayne. *Politics on the* Net: Wiring *the political process.* New York: Freeman, 1997.

Regan, Keith. “US: E-Commerce Topped $45B in 2002.” E-commerce Times, March 10, 2003. <http://www.ecommercetimes.com> (Date visited March 10, 2003).

Reich, M. (1990).*Origins of Terrorism*: *Psychologies, Ideologies, Theologies, States of Mind*. Cambridge: Cambridge University Press.

Schaffert, R.(1992). *Media Coverage and Political Terrorists*: *A Quantitative Analysis.* New York.

Smithsonian. “Birth of the Internet Timeline.” 2003. <http://smithsonian.yahoo.com/timeline.html> (Date visited: March 10, 2003).

Stern, J. (1999). *The Ultimate Terrorists*. Cambridge, MA: Harvard University Press.

Surratt, Carla. *Internet and Social Change*. London: McFarland and Company, Inc., 2001.

Tarrow, Sidney G. (1998). *Power in* Movement. Social *Movements and Contentious Politics, 2nd Ed*. New York: Cambridge University Press.

Tesar, Jenny. *Lifestyles and Pastimes.* New York: Macmillan, 1983.

Zaller, J. (1992). *The Nature and Origins of Mass Opinion*. New York: Cambridge University Press.

Zanini, Michele and Sean J.A. Edwards. “The Networking of Terror in the Information Age.” *Networks and Netwars*. Arquilla, John and David Ronfeldt. Ed. RAND: Santa Monica, 2001.

Author’s Note

Christopher Cox wishes to thank the following for their support in the completion of this project: Dr. Mary Borg of the Office of Undergraduate Academic Enrichment, University of North Florida for the financial assistance to complete this project, and Dr. Paul Harwood, for his patience and support throughout the duration of the independent study.