THE
TERRORISM RESEARCH
CENTER

For more information:
www.terrorism.com
trc@terrorism.com

Matthew G. Devost, Senior Analyst - Security Design International
Brian K. Houghton, Doctoral Fellow - RAND
Neal A. Pollard, Director of Research and Analysis - Hicks and Associates [1]

Information Terrorism: Can You Trust Your Toaster?

Scenario: September 1998

Tensions in the Balkan conflict have grown geometrically, particularly through Croat and Muslim aggression, with the failure of a series of peace accords. A new peace accord has been worked out, brokered by the United States, that stands a chance to redeem U.S. and NATO policy failures in the region, although some see it as harsher on Serbian combatants while it acquiesces to Croatian demands. Furthermore, NATO efforts at economic reconstruction have been particularly biased against Serbian interests. Determined to see its success in the face of flagging Congressional and public support for prolonging Bosnian operations, the President has increased the U.S. military presence in the region, establishing a new NATO airfield in Brcko, on the Bosnian/Croatian border, to facilitate logistics and put an end to the Balkan conflict. In September, with the prolonged fighting and the oncoming winter and its attendant fuel and food shortages and wave of refugees, stability in the region begins to deteriorate and

[1] The author's names are listed alphabetically to reflect that the research was conducted and implemented through a team effort with equal contributions. The opinions and conclusions contained herein are those of the authors, and do not reflect policy, institutional opinion, or proprietary information of their

Croat and Muslim troops increase activity; the President increases airlifts of troops and materiel, to counter tensions and support peace initiatives.

During the successive peace accord failures, and in response to increasing Croatian and Muslim aggression, sluggish economic recovery, and a tendency for NATO to be biased against Serbs, a group called the Serbian Council for the Liberation of Bosnia (SCLiB) is formed, consisting of Serb paramilitaries in Bosnia, Yugoslavia, and abroad, who have political and military influence among Yugoslavian and Bosnian Serb officials; the Council also consists of students in Slovenia, Hungary, and Yugoslavia, many of whom lost family members at the hands of Croats or NATO troops. The Council coalesced once members began to meet and communicate via the Internet, using PGP encryption to hide their interests and intentions. Their primary objective is revenge, to redress grievances from Croatian land usurpation and its support by their American patrons, and to rid the area of the NATO presence by dramatizing their cause to the people of the world, influencing them, and thus their governments, to demand NATO leave the area.

Having garnered enough financial and operational support through usual terrorist means, the Council formulates an attack, beginning with the CNN Web Page. By accessing the CNN Weather forecast, the Council times their attack for a night of intense storms in the Brcko area. Paramilitary members of the Council intrude on the frequencies of the approach and tower radios at the Brcko airfield: an airfield recently set up, and thus lacking ideal security measures, procedural experience, and full integration of NATO countries' respective military communications systems. In the

employers.

storm, flying into the airfield with its navigation lights off due to reported ground fire, a full C-130 troop transport is cleared to land by the approach intrusion. Another C-130, laden with fuel and also with its lights off, is cleared for take-off on the active runway, by the tower intrusion. The landing C-130 crashes into the second C-130. The resulting crash kills all aboard both planes. After hearing the explosion from their vantage point on a nearby hill, the intruders send a cellular signal to awaiting Council hackers in Slovenia. Upon receipt of the signal, the hackers immediately issue an "e-communiqué," taking responsibility for the crash, explaining how it was done, and giving the location of the intrusion equipment used, on which is engraved "SCLiB." The remainder of the message is their manifesto and claim for redress of grievances against life, property, and national identity. The end of the message is an invitation and address to access their Web site, which is actually run from a computer in Amsterdam by Slovenian foreign exchange students, via an anonymous web service account in Finland. This message is sent to and received by every major print and electronic news organization in the industrialized world, before the debris from the C-130 crash had settled.

The resultant publicity is astounding: CNN, Reuters, ITAR-TASS, and AP immediately broadcast the message, with the Web address. In addition, the e-communiqué itself was sent out to over 30,000 e-mail addresses in the first hour after the crash. Six minutes after the e-communiqué had been received, the Council Web page received its first hit.

Twenty-four hours after the C-130 crash, the Council Web had received over 1 million hits. The Web page was dramatic and rife with propaganda and claims against American, NATO, and Croatian imperialism and atrocities in the Balkan region, and *included questionable allegations of illegal arms transfers between NATO governments and Bosnian Muslims and Croats. Several references were included to the former U.S. presence in Lebanon, and how that presence was resolved. Twenty-four hours after the first hit, the first accessing system crashed, with all files irretrievably deleted, as a result of a Trojan horse the Council hackers had embedded in the Web page, exploiting a flaw in the programming language similar to one discovered by Princeton computer scientists in February 1996.*[2] *The flaw allowed a webmaster access to the hard drive and files of the machine that had unwittingly accessed the tainted Web page. Exploiting this flaw, the Council embedded a program that activated 24 hours (according to the system internal clock or any other time-keeping mechanism the machine could access) after the page was hit, destroying the functions and files of the system it infected. Although this created a sensational climate of fear throughout the computerized civilian world, the most damage done was to investigative and defense organizations, who immediately and naturally accessed the Web page before most of the news organizations had disseminated its address. This included the American Department of Defense, the Defence Ministries of all NATO countries, the American Department of Justice and Treasury, and the Central Intelligence Agency. Final damage to unclassified systems was incalculable, but the dramatization of the Council's cause was greatly effective. Since the Trojan horse was set to activate 24 hours after the Web site had been hit, computer failure rates tended to cascade, and were slow in tapering off, despite warnings to avoid the terrorists' Web page.*

[2] See http://www.cs.princeton.edu/~ddean/java/dns-scenario.html for the DNS attack scenario that Princeton researchers used to exploit a flaw in Java.

The actual reports of the carnage of the crash reached the public: these reports, on top of the fear created by the computer disasters, and the general frustration with American efforts in the Balkans, put enormous pressure on Congress and the President. Because of a lack of treaty conventions, American investigative agencies were not allowed to violate protocols of Finland's cyber-community; thus, investigators were unable to ascertain the identity of the anonymous server's customer, or the location of the Web site in Amsterdam. The Council's information terrorists remained secure in anonymity, and their success in hiding prompted many copy-cat web pages, a spate of "Internet liberators," and re-circulation of the Council's original manifesto and web page detail. With Congressional elections just over a month away, the Balkan mess became a rallying point of congressmen to pressure the President. Finally, the President had little choice but to accede to the public's and Congressional demands to bring the boys back home. Without American logistical and operational support, NATO's presence and power in the region was significantly reduced.

As with most conventional terrorist attacks, tactical damage to military and government information systems was relatively small (although several billion dollars of civilian and commercial information value could conceivably be lost in such a web-based attack). However, the strategic objective was not damage: as with most conventional terrorist attacks, the strategic objective was publicity, drama, and leverage to influence public and policy. The terrorists achieved their strategic objectives, clearly and effectively.[3]

[3] By a most unfortunate coincidence, this scenario was fully developed four days before the tragic crash of Commerce Secretary Brown's airplane in Croatia. While not wishing to exploit such a tragic loss, we feel

Introduction

In the remainder of the paper the authors will: 1) define information terrorism within the context of information warfare[4] as well as conventional terrorism; 2) offer a possible response to the phenomenon of information terrorism.

Information and Stability: The Lure of Technology

Extremist groups often resort to political violence when they lack the power to achieve political objectives through non-violent legal means. In an effort to attract the attention of the public, political terrorists perpetrate their acts with the media at the forefront of their strategy: this strategy calculus is based on the assumption that access to the communication structure is directly related to power.[5] Believers in this assumption might target digital information systems in pursuit of political goals.

The National Information Infrastructure (NII), and Global Information Infrastructure (GII) support financial, commercial and military information transfers for consumers, businesses, and countries. Considering the presence of computers in modern society, it is not surprising that terrorists have occasionally targeted computer systems in the past. A "PLO" virus was developed at Hebrew University in Israel; in Japan, groups have attacked the computerized control systems for commuter trains, paralyzing major cities for hours; the Italian Red Brigade's manifesto specified the destruction of computer

the scenario is still clearly relevant. Our most sincere condolences go to the families, friends, and colleagues of all who perished.

[4] For the purposes of this paper, “Information warfare” will be defined as offered by the Department of Defense: “Actions taken to preserve the integrity of one's own information system from exploitation, corruption, or destruction, while at the same time exploiting, corrupting, or destroying an adversary's information system and in the process achieving an information advantage in the application of force.” (Proposed: JCS Pub 1-02).

systems and installations as an objective for "striking at the heart of the state."[6] More recently, Sinn Fein supporters working out of the University of Texas, Austin, posted sensitive details about British army intelligence installations, military bases, and police stations in Northern Ireland on the Internet.[7] Terrorism is a rapidly evolving and responsive phenomenon. Terrorist technology and tactics are sensitive to their target political cultures, and have progressed at a rate commensurate with dominant military, commercial, and social technologies.

As technology becomes more cost-effective to terrorists--that is, its availability and potential for disruptive effects rise while its financial and other costs go down--terrorists may become more technologically oriented in tactics and strategies. In 1977, terrorist expert Robert Kupperman, then Chief Scientist of the U.S. Arms Control and Disarmament Agency, recognized that increasing societal reliance upon technology changes the nature of the threat posed by terrorists:

> Commercial aircraft, natural gas pipelines, the electric power grid, offshore oil rigs, and computers storing government and corporate records are examples of sabotage-prone targets whose destruction would have derivative effects of far higher intensity than their primary losses would suggest....Thirty years ago terrorists could not have obtained extraordinary leverage. Today, however, the foci of communications, production, and distribution are relatively small in number and highly vulnerable.[8]

The incorporation of information technology in the military-industrial complex, and the design and implementation of information warfare strategies, may also draw terrorists to computer technology. In the final days of the Cold War, NATO allies took

[5] See Alex P. Schmid & J.F.A. DeGraaf, *Violence as Communication: Insurgent Terrorism and the Western News Media*. Beverly Hills, CA: Sage, 1982.

[6] Philip Fites, Peter Johnson, & Martin Kratz, *The Computer Virus Crisis*, Second Edition. New York: Van Nostrand Reinhold, 1992 (p.63).

[7] *London Times*, via CNN Web News Digest, 26 March 1996 (http://www.cnn.com).

[8] Robert Kupperman, *Facing Tomorrow's Terrorist Incident Today*. Washington, DC: U.S. Department of Justice, Law Enforcement Assistance Administration, 1977. Cited in Grant Wardlaw, *Political Terrorism*, Second Edition. Cambridge: Cambridge University Press, 1989 (p.26).

seriously the premise that as warfare grows more electronic and dependent upon information technology, the vulnerabilities and risks of sabotage grow.[9] In a RAND paper, Dr. Bruce Hoffman asserts that, because of the operational conservatism resulting from the terrorists' "organizational imperative to succeed":

> ...terrorists will always seek to remain just ahead of the counter-terrorism technology curve: sufficiently adaptive to thwart or overcome the countermeasures placed in their path but commensurately modest in their goals (i.e., amount of death and destruction inflicted) to ensure an operation's success.
>
> In this respect, rather than attacking a particularly well-protected target-set or attempting high risk/potentially high payoff operations, terrorists will merely search out and exploit hitherto unidentified vulnerabilities and simply adjust their plan of attack and tactical preferences accordingly.[10]

Information technology offers new opportunities to terrorists with the above strategic concerns. In pursuing this *modus operandi*, a terrorist organization can reap low-risk, highly visible payoffs by attacking information systems.

Defining Information Terrorism

Information warfare has been examined within the context of state-on-state operations, as well as assessments of peer or near-peer competitors. However, sub-state and gray area[11] phenomena, especially information terrorism, have yet to be addressed within the paradigm of information warfare. Information warfare emanating from the low intensity end of the political violence spectrum represents a threat to American national security and defense.

[9] Gerald Segal, "Asians in Cyberia," *The Washington Quarterly*, v.18 n.3 (Summer 1995), pp.12-13.

[10] Bruce Hoffman, "Responding to Terrorism Across the Technological Spectrum," RAND Corporation, April 1994 (pp.29-30).

[11] "Gray-area phenomena" is political violence that is not easily seen to be sponsored by or connected to a state or an established organization.

An act of political violence by anyone other than a member of the armed forces of a legitimate state is often branded an act of terrorism. This is only occasionally correct[12], but the criminal and subversive connotations of the term "terrorist" have resulted in many acts of computer abuse being labeled "information terrorism." These acts have ranged from using personal information for extortion, to hacking into a network, to physical and/or electronic destruction of a digital information system. This is too simplistic a taxonomy for such a complex phenomenon.

Labeling every malicious use of a computer system "terrorism" serves only to exacerbate confusion and even panic among users and the general public, and frequently hinders prosecution and prevention by blurring the motivations behind the crime. Furthermore, political crimes have vastly different implications for national security and defense policy, than other "common" crimes. Terrorism is a *political* crime: an attack on the legitimacy of a specific government, ideology, or policy. Hacking into a system to erase files out of sheer ego, or stealing information with the sole intent to blackmail, is nothing more than simple theft, fraud, or extortion, and certainly is not an attack upon the general legitimacy of the government. Policy and methodology to counter crime depends a great deal upon criminal motivations;[13] thus, clearer and more concise definitions of "information terrorism" are needed, if it is to be addressed by national security policy. Attacks on the legitimacy of a government or its policies are not "common" criminal motivations. The quasi-criminal, quasi-military nature of terrorism blurs the distinction between crime and warfare. Distinctions between law enforcement and military duties

[12] For example, there is a distinct difference between terrorism and guerrilla warfare (See Walter Laqueur, *The Age of Terrorism.* Boston: Little, Brown & Co., 1987 [p.5]).

[13] This assumption is based on the notion that in political crimes, as opposed to crimes for ego or greed, the perpetrator and the beneficiary are usually not the same person, with more tenuous connections, and the intended long-term gains from the crime are usually abstract. From a law enforcement perspective, this places primacy on the motivations of the act; however, from a military perspective, it is the act itself which merits focus, since it is the act itself which wreaks the damage and poses the threat to national security. This is one of many facets in the argument surrounding the degree to which counterterrorism should be approached from a military *vis-à-vis* law enforcement perspective. This argument further emphasizes the need for a symmetrical, part-military part-law-enforcement response.

become equally blurred,[14] and can be clarified only through coherent policy dictating those duties, based upon a clear view of the nature of the enemy.

Political terrorism is the systematic use of actual or threatened physical violence in the pursuit of a political objective, to create a general climate of public fear and destabilize society, and thus influence a population or government policy. Information terrorism is the nexus between criminal information system fraud or abuse, and the physical violence of terrorism. However, particularly in a legal sense, information terrorism can be the intentional abuse of a digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action. In this case, the system abuse would not necessarily result in direct violence against humans, although it may still incite fear. Most terrorism scholars, when defining "political terrorism," would include physical violence as a necessary component; thus, many acts of criminal computer abuse would not be considered terroristic, if they do not result in direct physical violence. However, scholars must face the fact that as technology's implications broaden on society and politics, social and political definitions should likewise broaden to accommodate technology.[15] The semantic vacuum of a universally accepted comprehensive definition leaves room for considering information system abuse as a possible new facet of terrorist activity.

[14] Review of Richard Hundley and Robert Anderson, "Security in Cyberspace: An Emerging Challenge for Society," from *That Wild, Wild Cyberspace Frontier*. Internet source: http://www.rand.org/publications/RRR/RRR.fall95.cyber/wild.html, 5 April 1996.

[15] Stephen Sloan, "Terrorism: How Vulnerable is the United States?" Internet Source: *The Counter-Terrorism Page*, http://www.terrorism.com/Pubs/sloan.htm.

Tools and Targets

In a Third-Wave[16] society, there are two general methods in which a terrorist might employ an information terrorist attack: (1) when information technology is a target, and/or (2) when IT is the tool of a larger operation. The first method implies a terrorist would target an information system for sabotage, either electronic or physical, thus destroying or disrupting the information system itself and any information infrastructure (e.g., power, communications, etc.) dependent upon the targeted technology. The second method implies a terrorist would manipulate and exploit an information system, altering or stealing data, or forcing the system to perform a function for which it was not meant (such as spoofing air traffic control, as highlighted in the third scenario).

		Target	
		Physical	*Digital*
Tool	*Physical*	(a) Conventional Terrorism (Oklahoma City Bombing).	(b) IRA attack on London Square Mile, 4 October 1992.
	Digital	(c) Scenario (Radio intrusion in C-130 crash).	(d) Trojan horse in public switched network.

Figure 1

In the above matrix, cell (a) addresses "traditional" terrorism (e.g. hijacking, bombings, assassinations, hostage taking, etc.) The authors consider cells (b), (c), and (d) to be information terrorism. Cell (b) represents a low tech solution for a high tech target (e.g. the IRA attack on Square Mile financial district of London[17]). Cell (c) exploits information systems to wreak physical damage. Cell (d), digital tools against digital targets, exploits vulnerabilities in military, commercial and civilian/utility systems that rely

[16] Physical violence from terrorism uses Toffler's Second Wave technology, whereas information attacks would fall within the Third Wave paradigm. (See Alvin Toffler, *The Third Wave*. New York: Willam Morrow & Co., Inc., 1980.)

[17] The IRA were specifically targeting the Square Mile of London on a weekend to minimize casualties but maximize damage to a financial center of Western Europe.

on information technology. The authors believe cell (d) to be “pure” information terrorism and likely the most difficult to detect and counter.

No Symmetrical Response

A dilemma of combating terrorism in a democratic society is finding the right balance between civil liberties and civil security. Military operations within a democratic society, even to “protect” it, often are inconsistent with the principles of that society. The military thus confronts a paradox as it strives to combat terrorism. Although terrorists can use brutal, indiscriminate force against the military and civilian population, the military response may be limited. If the perpetrator of a terrorist action is found to be state-sponsored, a military response against state targets is possible (e.g. United States sending F-111s against Libya in response to Berlin Disco bombing in 1986).

Frequently terrorists are not state-sponsored, but are hidden within the civilian population. Tanks, aircraft and cruise missiles are ineffective against an enemy that blends itself into a civilian background. Information terrorists, outside the United States[18] have an easier means of disappearing inside their civilian population. Operating from homes[19] via modems, these terrorists can functions in their cell like structure using encrypted e-mail as means of communication to their organization’s network, and thereby reducing their chances of exposure.

The U.S. government faces this same paradox as it confronts information terrorism. Military, civilian and commercial databases, computer systems, information

[18] The authors chose to not to discuss domestic information terrorism, since that falls under the jurisdiction of the FBI, but much of the debate is similar regarding FBI capabilities to counter this threat.

infrastructures all are potential targets of information terrorists. Whether through digital or physical means, the information terrorists can destroy, disrupt, degrade, deny or delay vital information that the military relies upon, and thus become a threat in peace time, as well as in time of war. How can the U.S. national security establishment respond to the informational attacks of terrorists, when the terrorists hide behind a veil of digital anonymity? How much of information terrorism is a military concern and how much is within the jurisdiction of federal law enforcement?

The U.S. military could find it difficult to respond against a small and digitally networked enemy such as a terrorist campaign. The U.S. national security establishment needs to use a flexible, integrated response to counter information terrorists – one which employs information warfare tactics tailored to counter gray-area phenomena, but also reserves the use of conventional counter- terrorism operations.

Recommendations

The U.S. national security establishment must be equipped to respond militarily to information terrorism. Firstly, the military will always be a target of terrorism. Furthermore, the information terrorism attack may be state-sponsored and the first wave of a "digital Pearl Harbor." Origins of digital attacks are usually difficult to discover at first, and if the attack is indeed a precursor of peer or near-peer information warfare, a military response will be required.

[19] "Traditional" terrorists generally operate in an urban environment often without an established geographical locus. Information terrorism further diminishes geographical constraints through the nature of digital connectivity.

However, democratic societies must carefully weigh the use of military forces in the prevention and countering of terrorism, even though their militaries may be targets of the attacks. By calling in the military to respond to conventional terrorist actions, the terrorists and their cause may achieve a degree of legitimacy. The terrorists actions then have escalated from a criminal level to a "enemy of the state." This quandary can be avoided when countering information terrorists. There are no visible soldiers on the streets to heighten civilian anxieties when using digital attacks to counter the terrorists. The military's response, like that of the information terrorists, can be anonymous, fully networked, and swift.

The military has unique capabilities to confront and counter international information terrorism which the domestic law enforcement agencies lack, particularly in the military's specialized training and established international presence. Aspects of an international information terrorist attack (especially within cell (d) [see Figure 1]) would fall squarely within the jurisdictions of several federal law enforcement agencies because these attacks would affect a domestic information system, just by virtue of the connectivity of such systems. Furthermore, the investigative abilities of law enforcement agencies such as the FBI and the Treasury Department's FinCEN (Financial Crimes Enforcement Network) are particularly well-suited to counter information terrorism, from detecting the logistics and method of attack to following the money trail and uncovering a possible sponsor. The most important aspect of any counter terrorist endeavor is a rapid response time. Law enforcement is particularly adept at rapid crisis management. Clearly, the ideal response structure would be one that incorporates assets from both the military and law enforcement. Such a structure could also incorporate the military in an advisory role in domestic incidents, and likewise, law enforcement assets in an advisory role in overseas incidents.

Offensive information warfare techniques developed for military use at a state level could also be utilized to respond to information terrorism. Law enforcement agencies, in general, do not have similar offensive information warfare capabilities. For this reason a specialized and integrated counter information terrorism group is required. These highly trained information warriors would be the national security equivalent of Carnegie Mellon's Computer Emergency Response Team, but with an offensive capability. Like a "Digital Delta Force" these Digital Integrated Response Teams (DIRTs) would work from remote computer systems and use information warfare tactics to detect, locate and counter the information terrorists. The DIRTs would be in networked remote cells inside CONUS (with one on the East and West coasts, and an additional cell in the Midwest). The DIRTs would exploit law enforcement IT-oriented assets, investigative capabilities, and intelligence bases. The DIRTs, created by Executive Order, would operate as a cell of the National Security Council and take its directives from the information terrorism counterpart to the White House "Drug Czar."

These information warriors, comprised of members from the Joint Services, as well as Justice and Treasury Departments, would strike using digital means against computers and networks used by the information terrorists. Using an anonymous response, the U.S. government could strike at information terrorists without large display or legitimizing the terrorists, both of which would occur with a physical response. Such a response offers ultimate plausible denial. In addition, the DIRTs close integration with law enforcement agencies would provide legal guidance and accountability, and avoid a “Posse Comitatus” syndrome.

This structure would combine the investigative and jurisdictional assets of the law enforcement community with the offensive capabilities of the military. If the United States is going to enter the Information Age, we need to have policy that spans the spectrum of information-related threats to our national security, driving offensive *and* defensive assets that can respond symmetrically and effectively. Our offensive capabilities against peer or near-peer competitors are formidable, whether in information or conventional warfare. However, the integration of law enforcement assets are necessary to respond effectively to a networked gray-area attack. Without an integrated, fully articulated response policy, information terrorists could severely damage the infrastructures of our military or society, in the time it takes to argue about whose job it is to respond.

13 April 1996